

Convenio de colaboración entre a Consellería de Infraestruturas e Mobilidade e a empresa PROCONSI, SL, mediante o que se instrumentaliza a compensación á devandita empresa pola adaptación informática das máquinas canceladoras comercializadas por ela á integración dos códigos QR nas tarxetas TMG Xente Nova, no marco do Plan de Transporte Metropolitano de Galicia.

REUNIDOS

Dunha parte, **Ignacio Maestro Saavedra**, director xeral de Mobilidade, actuando por delegación da conselleira de Infraestruturas e Mobilidade, de acordo co establecido na Orde do 7 de setembro de 2017 sobre delegación de competencias no secretario xeral técnico e noutros órganos e entidades públicas adscritos a esta consellería (DOG Núm. 179, do 20 de setembro).

Doutra parte, **Constantino Lázaro de la Osa**, con DNI número 12399251C, actuando en nome e representación da empresa PROCONSI, S.L. con CIF número B24208100, de acordo coa escritura pública de outorgamento de poder inscrita no rexistro mercantil de León.

As partes recoñécense mutuamente capacidade e competencia para formalizar este acordo, e, para tal efecto,

EXPOÑEN

1. A Xunta de Galicia, xunto coas administracións municipais das principais áreas urbanas de Galicia, puxo en marcha o Plan de transporte metropolitano de Galicia (PTMG), consistente nun conxunto de programas dirixidos a potenciar a utilización do transporte público colectivo, medidas que foron reforzadas a partir do ano 2016 coa implantación dunha tarifa específica dirixida ás persoas menores, naquel momento, de 19 anos, a tarifa Xente Nova.

Posteriormente, como consecuencia da aprobación do Plan de Transporte Público de Galicia (PTPG), xeneralizáronse ao conxunto da Comunidade Autónoma diferentes actuacións no ámbito das tarifas e bonificacións aplicables nos servizos públicos de transporte.





Entre estas actuacións, ampliouse tanto o abano de idades das persoas que se favoreceron pola tarifa *Xente Nova*, ao incluír á poboación abranguida entre os 4 e os 20 anos incluídos (Orde da Consellería de Infraestruturas e Mobilidade, do 18 de decembro de 2019; DOG nº 248, do 31 de decembro); e tamén se procedeu á extensión do ámbito de aplicación desta tarifa ao conxunto do territorio da Comunidade Autónoma (*Resolución do 6 de maio de 2021, da Dirección Xeral de Mobilidade, pola que se culmina o procedemento de expansión do ámbito territorial de aplicación da tarifa específica XN ao conxunto do transporte público da competencia da Xunta de Galicia*; DOG núm. 93, do 20 de maio), de xeito que a tarifa *Xente Nova* xa é aplicable para calquera viaxe interurbana que se realice nos servizos públicos de transporte regular de uso xeral da competencia da Comunidade Autónoma de Galicia.

Para a xestión da dita tarifa *Xente Nova* é preciso a utilización dunha tarxeta moedeiro, prepagamento e nominativa, de tal forma que a persoa usuaria realiza o pagamento das viaxes por adiantado e, con posterioridade, a Xunta de Galicia reintégrralle o importe pagado.

Ademais, dada a aceptación e as vantaxes que para a mocidade representa esta tarifa *Xente Nova*, anualmente veuse acordando darlle continuidade ao seu prazo de vixencia; así, na actualidade, está vixente a *Resolución do 25 de novembro de 2022, da Dirección Xeral de Mobilidade, pola que se amplía o prazo de vixencia da tarifa específica Xente Nova no transporte público interurbano da competencia da Xunta de Galicia para o ano 2023* (DOG núm. 231, do 5 de decembro).

2. Dende o punto de vista técnico, o funcionamento dos programas do PTPG require da instalacións dunhas máquinas canceladoras a bordo dos medios de transporte que prestan os seus servizos no territorio da Comunidade Autónoma de Galicia. Estas máquinas canceladoras deben cumprir unha serie de especificacións técnicas para garantir a seguridade da remisión dos datos das colectas ao sistema informático de xestión (SITME) e á entidade colaboradora (actualmente ABANCA).

Con motivo da implantación do denominado Novo PTMG, no que se incorporou a tarxeta TMG, no ano 2010 levouse a cabo unha labor de adaptación das máquinas canceladoras empregadas polas concesións de servizos públicos de transporte de Galicia, sendo obxecto da súa



homologación por parte de ABANCA e dos servizos tecnolóxicos da Xunta de Galicia.

Actualmente, existen no mercado varias máquinas canceladoras homologadas para o seu funcionamento no PTPG, entre as que figura o equipamento desenvolvido por PROCONSI, SL.

3. As medidas promovidas pola administración autonómica dirixidas a mellorar a utilización do sistema de transporte público requiren de medios tecnolóxicos axeitados para a súa xestión, mais resulta esencial a constante evolución destes sistemas, para a fin de adaptalos á propia evolución da tecnoloxía e da súa utilización e aceptación por parte da poboación. Neste sentido, na actualidade a Xunta de Galicia pretende avanzar neste proceso mediante a *virtualización* da TMG *Xente Nova*, de xeito que non se habilite o pagamento directamente cun teléfono móbil e sen necesidade de adiantar o importe das viaxes, todo isto mediante a utilización un código QR e a súa lectura e procesamento polo sistema tecnolóxico.

A finalidade é ofrecer unha alternativa electrónica á tarxeta física para estender o uso da tarxeta TMG *Xente Nova*, evitando os desprazamentos dos usuarios ás sucursais bancarias para a súa recarga e a aceptación dos reintegros.

Para a implementación deste novo modelo de TMG *Xente Nova* “*virtual*”, será precisa unha adaptación das máquinas canceladoras utilizadas nos medios de transporte, adaptación que deben realizar as empresas comercializadoras das mesmas.

Tendo en conta a natureza deste proxecto, como iniciativa da Administración, e o seu interese na correcta e máis áxil implementación, e tendo en conta a obriga concesional de que os equipamentos de cancelación contén cun lector de códigos QR (*hardware*), a adaptación tecnolóxica a desenvolver afectará ao *software* que deberá utilizar a máquina e o propio lector, desenvolvemento que non se considera viable trasladar ás empresas concesionarias dos servizos públicos de transporte, polo que a Consellería de Infraestruturas e Mobilidade prevé celebrará convenios coas empresas provedoras dos ditos equipamentos para a súa adaptación coa finalidade de que as máquinas canceladoras poidan procesar as cancelacións da TMG *Xente Nova* “*virtual*” a través da lectura e procesamento dun código QR





dinámico, e aplicar unha lóxica de negocio, asumindo o custo íntegro deste desenvolvemento.

4. Mediante o presente documento instrumentalízase a colaboración entre a empresa PROCONSI, SL, e a Consellería de Infraestruturas e Mobilidade para o desenvolvemento do *software* aplicable en todas as máquinas canceladoras do Transporte Público de Galicia, comercializadas polo dito provedor, de xeito que integren as funcionalidades precisas para a xestión da nova TMG *Xente Nova* "virtual", con lectura de código QR.

Considerando o interese público concorrente na adaptación dos sistemas e a súa posta a disposición das empresas concesionarias dos servizos públicos de transporte regular de viaxeiros de uso xeral por estrada do xeito máis áxil posible, prevese o convenio de colaboración como o instrumento máis axeitado.

Consonte co anterior, as administracións asinantes

ACORDAN

Asinar este convenio, e obrigarse reciprocamente ao seu cumprimento, de conformidade coas seguintes

CLÁUSULAS

PRIMEIRA. OBXECTO

O presente convenio ten por obxecto a adaptación informática das máquinas canceladoras comercializadas por PROCONSI, S.L., implantadas en servizos públicos de transporte regular de viaxeiros, mediante o desenvolvemento do *software* aplicable e requirido para a integración da funcionalidade de tarxetas TMG *Xente Nova* virtual con lectura e procesamento de códigos QR, no marco do Plan de Transporte Público de Galicia.

SEGUNDA. PRESTACIÓNS E FINANCIAMENTO

1. A empresa participante no presente convenio deberá realizar as seguintes prestacións:

1ª) Modificacións no *software* das máquinas canceladoras.





- Integración do lector de QR na lóxica do *software* de billeteaxe, lectura e interpretación dos datos do QR e validación básica.
- Validación criptográfica.
- Creación e uso da lista negra local.
- Función de anulación do pagamento con QR.
- Sinalética da operación.
- Tickets ao viaxeiro.
- Notificación de validacións de QR Xente Nova ao servidor do SAE particular.

2ª) Novas funcións a nivel do servidor do SAE particular.

- Recepción das operacións de QR desde as máquinas canceladoras.
- Comunicaci3ns ao API Xente Nova QR.
- Comunicaci3ns co SITME.

3ª) Probas e homologaci3ns.

4ª) Despregue da aplicaci3n e formaci3n dos operadores.

5ª) Todos os traballos precisos para a correcci3n de erros durante o prazo dun ano desde o despregamento da aplicaci3n, a3nda que estes erros non sexan responsabilidade da empresa participante no presente convenio.

2. O proceso de homologaci3n das empresas constar3 de d3as fases:

1ª) A fase de homologaci3n no laboratorio.

Facilitarase a PROCONSI, SL. unha versi3n de probas da APP de transporte p3blico de Galicia e un plan de probas que deber3 executar sobre unha m3quina adaptada nun entorno de laboratorio. Como resultado das devanditas probas deber3 remitir 3 Direcci3n Xeral de Mobilidade, dependente da Conseller3a de Infraestruturas e Mobilidade, o plan de probas cuberto, coas probas realizadas e o resultado das mesmas, as3 como unha colecta que integre as operaci3ns realizadas.

Unha vez revisados, se os resultados son satisfactorios realizar3ase o mesmo plan de probas con outros casos de proba diferentes.

2ª) Fase piloto.





Superada a fase inicial de homologación en laboratorio, para conseguir a homologación final será preciso completar unha fase piloto en dous autobuses nos que se realizarán validacións coa APP QR Xente Nova de produción. As operacións QR Xente Nova enviaranse a través do SITME en colectas v6 xunto co resto de operacións con TMG e en efectivo.

3. O prazo máximo para a superación do proceso de homologación completo é de ata seis meses, debendo rematar, en todo caso, **non máis tarde do 23 de decembro de 2023**.

4. Polos traballos de adaptación das máquinas canceladoras indicadas, a Consellería de Infraestruturas e Mobilidade comprométese a abonar á empresa participante no presente convenio o importe do gasto no que incorrese para a realización dos desenvolvementos que se prevén no presente convenio, ata o máximo de **trinta e tres mil trescentos noventa e seis euros (33.396 €), IVE incluído**, que será financiado con cargo á aplicación orzamentaria 2023.09.02.512A.470.1 dos orzamentos xerais da Comunidade Autónoma de Galicia no exercicio 2023.

5. Os importes correspondentes aos desenvolvementos que se prevén nesta cláusula, que teñen o carácter de máximos, serán abonados por parte da Consellería de Infraestruturas e Mobilidade logo de que por parte da empresa participante no convenio se certifique a súa completa realización e se achegue a xustificación do correspondente gasto, incluído, no seu caso, o gasto no que se incorrera con medios propios, certificación e xustificación que terá que ser remitida á Dirección Xeral de Mobilidade non máis tarde do **23 de decembro de 2023**.

TERCEIRA. OUTROS REQUISITOS

As especificacións técnicas e os desenvolvementos a implementar recóllense no anexo I do presente convenio. Pola súa parte, no anexo II especificase o novo formato de colecta v.6.

A dita información incorpórase para efectos informativos, debendo estar para a execución dos traballos de desenvolvemento e adaptación, en todo caso, á resultante dos documentos técnicos elaborados por AMTEGA e comunicados á entidade comercializadora parte neste convenio.



CUARTA. VIXENCIA

Este convenio terá vixencia durante un ano a contar desde a súa formalización.

En calquera momento antes da finalización do indicado prazo, as partes poderán acordar a súa prórroga por un período dun ano mediante a sinatura do correspondente acordo.

Non obstante, calquera das partes poderá desistir do convenio comunicándoo de maneira fidedigna ás outras cunha antelación mínima de tres meses.

QUINTA. OBRIGAS DAS PARTES E DEBER DE CONFIDENCIALIDADE

1. A empresa participante no presente convenio deberá presentar a certificación do proceso de homologación realizado, sendo preciso que se poida verificar pola Dirección Xeral de Mobilidade ou, por indicación desta, pola AMTEGA, que se levou a cabo. Na certificación deberán comprometerse a actualizar o software de todas as máquinas canceladoras do Transporte Público de Galicia subministradas pola dita entidade comercializadora, sen custo ningún para as empresas operadoras, co sistema de *software* preciso para a integración do lector de código QR na lóxica do *software* de billeteaxe, lectura e interpretación dos datos do QR e a validación, nos termos indicados nos anexos deste convenio e, no seu caso, nos documentos técnicos que lle teñan sido facilitados por parte da AMTEGA.

A dita certificación **presentarase, a máis tardar, o 23 de decembro de 2023**, xunto con tanta documentación resulte precisa para o pagamento do importe previsto nos apartados cuarto e quinto da cláusula segunda deste convenio.

2. PROCONSI, SL, comprométese a formar aos operadores e a realizar todos os traballos necesarios para a corrección de erros que afecten á operativa dos desenvolvementos que son obxecto deste convenio, durante o prazo dun ano desde o despregue da aplicación, aínda que estes erros non sexan responsabilidade de PROCONSI, S.L.

3. A Consellería de Infraestruturas e Mobilidade comprométese ao pagamento do importe máximo indicado na cláusula segunda, unha vez superado o proceso de homologación pola empresa participante no presente





convenio, e trala presentación da certificación e xustificación esixida no apartado 1 da presente cláusula, e na mencionada cláusula segunda.

4. Cada unha das partes comprométese a cumprir, no ámbito de execución do presente Convenio, coas obrigas e deberes que respectivamente lles correspondan, de conformidade co disposto no Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos (en diante, "RXPD"), así coma na Lei Orgánica 3/2018, do 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais (en diante, "LOPDXDD") e en calquera normas aplicables ou que no futuro poidan promulgarse en desenvolvemento da anterior.

SEXTA. COMISIÓN DE SEGUIMIENTO

Establécese unha comisión mixta de seguimento deste convenio, á que serán sometidas as cuestións que expresamente se prevén no mesmo así como aquelas outras que deriven do desenvolvemento deste acordo aínda que non estean expresamente recollidas nel, así como aquelas que impliquen desconformidade por algunha das partes asinantes.

Esta comisión está composta por:

- Pola Consellería de Infraestruturas e Mobilidade, o director xeral de Mobilidade ou a persoa en quen delegue, que a preside.
- Por PROCONSI, SL, Constantino Lázaro de la Osa, ou persoa en quen delegue.
- Actuará como secretario ou secretaria unha ou un funcionario da Dirección Xeral de Mobilidade.

A persoa representante de PROCONSI, SL. poderá ser substituída por quen deteña a representación legal da dita empresa, previa comunicación formal da dita substitución á secretaría da dita comisión.

SÉTIMA. NATUREZA XURÍDICA E NORMATIVA APLICABLE

Este convenio atópase incluído dentro dos previstos no artigo 6.2 da Lei 9/2017, de 8 de novembro de 2017, de contratos do sector público, polo que queda fóra do ámbito de aplicación desta lei. Non obstante, aplicaranse os



principios desta norma para resolver as dúbidas ou lagoas que puidesen presentarse.

Este convenio rexerá polas súas cláusulas e pola Lei 40/2015, do 1 de outubro, de réxime xurídico do sector público, así como polas disposicións que en materia de convenios se recollen na Lei 1/2016, do 18 de xaneiro, de transparencia e bo goberno da Xunta de Galicia.

OITAVA. RELACIÓNS COA CONSELLERÍA DE INFRAESTRUTURAS E MOBILIDADE

A subscrición do convenio non implicará relación laboral, contractual ou de calquera outro tipo entre os profesionais que realicen as actividades obxecto daquel e a Consellería de Infraestruturas e Mobilidade, de xeito que non se lle poderá esixir a esta responsabilidade ningunha, nin directa nin subsidiariamente, polos actos ou feitos ocorridos durante o seu cumprimento.

NOVENA. TRANSPARENCIA E PUBLICIDADE

Este convenio será obxecto de publicación nos termos do artigo 15 da Lei 1/2016, do 18 de xaneiro, de transparencia e bo goberno e demais normativa aplicable, e as partes manifestan o seu consentimento para que os datos persoais que consten no convenio, e mailo resto das especificacións contidas neste, poidan ser publicadas no Portal de Transparencia e Goberno Aberto.

DÉCIMA. CAUSAS DE RESOLUCIÓN

Este convenio poderase resolver por calquera das seguintes causas:

- a) O incumprimento total ou parcial dalgunha das cláusulas reguladoras. Para estes efectos, calquera das partes poderá denunciar por escrito o convenio, trasladándollo de maneira fidedigna ás outras cunha antelación mínima de dous meses á data prevista para a resolución.
- b) O transcurso do prazo de vixencia sen terse acordado a prórroga do mesmo.
- c) O acordo das partes asinantes.





E para que conste, en proba de conformidade, os comparecentes asinan dixitalmente este convenio na data indicada nas correspondentes sinaturas dixitais.

Pola Consellería de Infraestruturas e
Mobilidade

PD (Orde do 07/09/2017; DOG Núm. 179, do 20 de setembro)

Por PROCONSI, S.L.

Constantino Lázaro de la Osa

Ignacio Maestro Saavedra

ANEXO I

Documento de especificacións técnicas



QR XENTE NOVA

Integración provedores expendedoras

CLÁUSULA DE CONFIDENCIALIDADE

Este documento é propiedade da AMTEGA (Axencia para a Modernización Tecnolóxica de Galicia). Deberá empregar este material exclusivamente para os servizos que foron acordados coa AMTEGA e que requiren necesariamente da súa utilización. Está prohibida a reprodución parcial ou total, por calquera medio ou método, dos contidos deste documento para calquera outro uso non acordado coa AMTEGA.



1. Alcance

O presente documento identifica o conxunto de especificacións a cumprir para que os provedores de expendedoras do Transporte Público de Galicia se poida integrar no sistema QR XenteNova.

2. Introducción

A tarxeta Xente Nova é unha tarxeta física propiedade de Amtega e Abanca coa mesma estrutura interna que a tarxeta TMG. O seu uso está acoutado a menores de 21 anos, debendo a persoa usuaria acudir a Abanca para solicitar a tarxeta de transporte de Galicia e, se cumpre a condición de ser menor de 21 anos, Abanca facilítalle a tarxeta Xente Nova en lugar da tarxeta TMG.

O seu funcionamento é idéntico ao da tarxeta TMG coa excepción de que a Xunta de Galicia, a través de Abanca, abona os billetes previamente pagados pola persoa usuaria; o dito aboamento efectúase mediante unha recarga que a persoa usuaria pode facer efectiva nun caixeiro na segunda quincena posterior á da viaxe (postpago de Abanca á persoa usuaria). É dicir, a persoa usuaria debe validar a tarxeta Xente Nova nas máquinas expendedoras homologadas por Abanca /Amtega sempre e cando teña saldo, xa que na validación descóntaselle o importe de forma idéntica á tarxeta TMG.

O Sitme, pola súa banda, ao recibir nas colectas as operacións procedentes dos sistemas de ticketing das empresas concesionarias calcula o importe abonado pola persoa usuaria, trasládallo á Dirección Xeral de Mobilidade que, a través de ABANCA pon ao dispor da persoa usuaria a recarga correspondente nun caixeiro automático, devolvéndolle así o importe previamente abonado por ela.



Tarxeta física Xente Nova





3. Integración no sistema XenteNOVA QR

3.1. Consideracións previas

Neste apartado inclúese aquela información que deba coñecerse de antemán.

3.1.1. Formato data-hora

Todas as data-hora son UTC, cada dispositivo débea transformar á zona horaria que teña configurado. O formato co que se compón a data e hora é o seguinte:

32 bits, en orden de esquerda a derecha.

A	A	A	A	A	A	M	M	M	M	D	D	D	D	D	H
H	H	H	H	N	N	N	N	N	N	S	S	S	S	S	S

A – Ano (6 bits): este valor son os anos transcorridos dende o ano 2000.

M – Mes (4 bits)

D – Día (5 bits)

H – Hora (5 bits)

N – Minutos (6 bits)

S – Segundos (6 bits)

Exemplo. De hexadecimal a data ->594AF790 = 05/05/2022 15:30:16

3.2. Definición do QR

A APP xera un QR como pode ser o seguinte:



Este QR ten unha lonxitude de 228 bytes e está en formato base64. Disto dedúcese que unha primeira comprobación do QR lido é dita lonxitude e formato, xa que a codificación base64 só admite os seguintes caracteres: a-z, A-Z, 0-9, +, = y /. Decodificando base64, obtense o seguinte:





BASE64:

AAEAAACPAAAAAwEAAABsAAABBB1yiAABco277AAEAtAABF9m07ZMhkkETmliDtn9
nhyFA6kIIlp3D2ZKqg4QZ4ZEa8yxQVJhmuTKnK8Gy6JchwsqCvdn7vCD7x4gDbNve
KT/wq7E4RbWSCZ+vEe9g2lwtXXOBtUpr3WSxiDtDst1kt8z8TXCvui+KDnQUAyV/Kof
7N7ELmTYdczE0dvW6NdU2KXGXIUzmzRQ==

HEX:

00010000008F00000003010000006C000001075CA200005CA36EFB000100B400
0117D9B4ED9321924113988883B67F67872140EA42252E9DC3D992AA838419E1911A
F32C50549866B932A72BC1B2E89721C2CA82BDD9FBBC20FBC788036CD55E293FF0
ABB13845B592099FAF11EF60DÁ5C2D5D7381B54A6BDD64B1883B43B2DD64B7CCF
C4D70AFBA2F8A0E741403257F2A87FB37B10B99361D73313476F5BA35D536297197
9549B345

Morado = Parte estática do QR (33 bytes).

Azul = Parte de autenticación do QR (128 bytes).

Verde = Parte dinámica do QR (8 bytes).

Campo	Bits	Rango	Valor exemplo (HEXA)
Parte estática			
Versión QR	8	0-255	00
Tipo QR	8	0-255	01
Identificador QR	32	0-FFFFFFFF	0000008F
Identificador conta	32	0-FFFFFFFF	00000003
Tipo orixe e destino	8	0-255	01
Orixe	32	0-FFFFFFFF	0000006C
Destino	32	0-FFFFFFFF	00000107
Data-hora de inicio de validez	32	0-FFFFFFFF	5CA20000
Data-hora de remate de validez	32	0-FFFFFFFF	5CA36EFB
Saldo	16	0-65535	0001
Validez dinámica (en segundos)	16	0-65535	00B4
IDE clave asina	16	0-65535	0001





Parte de autenticación			
Sinatura	1024		17D9B4ED9321924113988883B67F67872140EA 42252E9DC3D992AA838419E1911AF32C50549 866B932A72BC1B2E89721C2CA82BDD9FBBC2 0FBC788036CD55E293FF0ABB13845B592099F AF11EF60DÁ5C2D5D7381B54A6BDD64B1883B 43B2DD64B7CCFC4D70AFBA2F8A0E74140325 7F2A87FB37B10B99361D73313476F5BA35D5
Parte dinámica			
Data-hora xeración/refresco	64	0- FFFFFFFFFFFF FFFF	362971979549B345

3.3. Parte estática do QR

A parte estática do QR é a parte na que os datos son fixos relativos á viaxe e non poden cambiar.

- **Versión QR:** Chegará sempre 00.
- **Tipo QR:** Chegará sempre 01.
- **Identificador QR:** identificador único para cada código QR.
- **Tipo orixe e destino:** Chegará sempre 01, que significa "concello".
- **Orixe:** Se tipo orixe e destino é 01, é código de concello orixe do Sitme.
- **Destino:** Se tipo orixe e destino é 01, é código de concello destino do Sitme.
- **Data e hora de inicio de validez:** data-hora a partir da cal se pode validar o QR.
- **Data e hora de remate de validez:** data-hora a partir da cal xa non se pode validar o QR.
- **Saldo:** Número de viaxes dispoñibles na conta do usuario.
- **Validez dinámica:** indica o número de segundos que faltan ata o usuario deba rexenerar o QR na APP coa data e hora da parte dinámica actualizada.
- **ID clave asina:** Identificador que indica a clave para utilizar para verificar a sinatura.

3.4. Parte de autenticación do QR



A parte de autenticación do QR serve para verificar a autenticidade do QR

- **Sinatura:** é o hash SHA-256 da parte estática do QR, encriptado usando RSA. No apartado do proceso de autenticación do QR explícase con detalle.

3.5. Parte dinámica do QR

Contén data-hora de xeración do QR encriptada con TDES. No apartado do proceso de autenticación do QR explícase con detalle.

- **Data-hora de xeración/refresco do QR:** data-hora na que se xerou/refrescou o QR.

3.6. Notificación de validacións.

As validacións comunicaranse ao backoffice sempre o antes posible, para que a conta do usuario se actualice no menor tempo posible; para iso habílanse tres vías para notificar a realización dunha validación:

- Notificación dunha validación en tempo real, ou quasi tempo real a través do backoffice do provedor/empresa de transporte. (Con política de reintentos)
- Notificación de varias validacións desde o backoffice do provedor/empresa de transporte.
- Notificación de validacións a través do Sitme. (Impleménteo ao Sitme tras procesar as colectas).

Nótese que, no caso de non ter conexión desde a expendedora coa API, o QR (validación offline) débese dar por válido se cumpre as condicións de validación na expendedora e notificarase a posteriori ao sistema QR XenteNova (política de reintentos na expendedora), e a través do backoffice da empresa de transporte e a través do Sitme (consolidación da operación).

4. Notificación de operacións a API XenteNova

4.1. Notificación desde a expendedora

As operacións con QR realizadas nas expendedoras hanse de remitir en tempo real (permítese pasar polo backoffice do provedor/empresa de transporte) á API Rest XenteNOVA QR para o seu procesado e actualización das contas de usuario.





As chamadas á API realízanse mediante usuario e contrasinal que subministrará o equipo de soporte do proxecto na Amtega. A url á que notificar o resultado da operación con QR realizadas nas expendedoras (validación/anulación/erros) será subministrado polo equipo de soporte do proxecto na Amtega.

Para realizar unha chamada á API, é necesario autenticarse seguindo o estándar JWT, para obter un *token* valido hai que realizar unha chamada ao *endpoint* `/api/Login/authenticate` indicando no corpo da petición o usuario e contrasinal, en formato JSON:

```
{
  "username": "string",
  "password": "string"
}
```

Débese establecer unha política de reintentos na expendedora para que, no caso de problemas de comunicación (falta de cobertura), se envíe a notificación de que un QR se validou o antes posible ao recuperar a cobertura.

O obxectivo desta notificación en tempo real desde a expendedora (ou en tempo real pasando polo backoffice do provedor da expendedora) é que o backoffice de XenteNova QR este informado o antes posible de que se realizou a validación do QR.

O formato do método para notificar as validacións está recollido na seguinte táboa:

Parámetros ao método da API para enviar validación QR





Notificar operacións QR			
Endpoint	POST /api/Qr/validation		
Parámetros do DTO petición	Nome	Tipo	Descrición
	IdQr	int	Identificador único de cada código QR. Dato do QR
	IdAccount	int	Identificador único de cada conta de usuario que utiliza o QR. Dato do QR.
	IdProvider	int	Identificador do provedor de expendedoras desde o que se realiza a validación do QR. Neste campo ponse o identificador do provedor (GMV, Olton, Proconsi e IST) que está a notificar a validación do QR.
	IsRealTime	boolean	Flag para indicar se a transacción é en tempo real, é dicir, se se está enviando esta transacción no momento no que se validou o QR. Provedores de expendedoras cubrir con True.
	IdEquipment	int	Identificador do equipo que realiza a validación. Nº de serie expendedora.
	TicketSerialNumber	String	Nº de serie do billete validado ou anulado. Ej. AA12345. Dato expendedora.
	OperationDateTime	DateTime	Data e hora da validación/anulación/transbordo. Ej: 2022-09-01T15:09:29. Dato expendedora.
	IdFare	int	Identificador da tarifa. N/A. Cubrir con 0.
	Price	int	Prezo do billete equivalente TMG. Neste caso ten dous decimais implícitos no valor. Por exemplo , para 1,5 € represéntase en enteiro como 150, con dous decimais implícitos á dereita. Dato expendedora.
	IdRoute	int	Identificador da liña de autobús onde se realizou a operación. Id_Linea Sitme. Dato expendedora.
	IdLine	int	Identificador do traxecto de autobús onde se realizou a operación. IdRutaSitme*10+Sentido. Dato expendedora.
	IdExpedition	int	Identificador da expedición onde se realizou a operación. Id_Expedicion Sitme. Dato expendedora.
	IdVehicle	string	Identificador do vehículo onde se realizou a operación (Matricula) Dato expendedora.





	IdDriver	int	Código do condutor no que se realizou a operación. Dato expendedora.
	IdOriginStop	int	Identificador da parada onde se realizou a operación. Id_paradaSitme. Dato expendedora.
	IdOrigin	int	Identificador da orixe, que non é parada, onde se realizou a operación. Neste caso trátase do identificador do Sitme do concello orixe. Dato expendedora.
	IdDestinationStop	int	IdparadaSitme. Dato expendedora. Identificador da parada destino, que sería a última parada do traxecto onde se realizou a operación.
	IdDestination	int	Identificador do destino. Neste caso trátase do identificador do Sitme do concello destino. Dato expendedora.
	OperationType	int	Identificador do tipo de operación. 1 – Validación de QR 25 – Anulación de validación 100 – Erro Dato expendedora.
	OperationResult	int	Identificador do resultado da operación. 0 – Validación OK 1 – QR caducado 2 – QR Passback 3 – QR erro Orixe-Destino 4 – QR erro formato Dato expendedora.
	Signature	String	Sinatura do QR. É un valor de 128 bytes, polo que se pasa como String representando a cadea de bytes en hexadecimal. Dato QR



Exemplo de
notificación de
QR validado
correctamente
en
expendedora

```
{
  "idQr": 28,
  "idAccount": 1,
  "idProvider": 1,
  "isRealTime": true,
  "idEquipment": 6555,
  "ticketSerialNumber": "string",
  "operationDateTime": "2022-09-01T15:09:29",
  "idFare": 0,
  "price": 88,
  "idRoute": 1524,
  "idLine": 11,
  "idExpedition": 99584,
  "idVehicle": "1255LDB",
  "idDriver": 1,
  "idOriginStop": 257,
  "idOrigin": 1,
  "idDestinationStop": 38764,
  "idDestination": 108,
  "operationType": 1,
  "operationResult": 0,
  "signature":
    "1CEC8A9C9752D10A72D55EC2A3A8B5E414AAE2ED6597964E77251DC21764BC35EBBC6C
    7FD2F2BFC515564D9A4AA76BC54AFE0C64091881027F8E17CFD580945E5475259CE2F570
    668A12D856FC25C05C8EED96DÁ3F03FEC49C591B670075F3327CA13F33ED00289F251840
    20E25E8027C1FC5CAB6B8A3A7CA7ECB298503E"
}
```

4.1.1. Respostas da API á notificación dunha validación

Nunha primeira etapa do proxecto a API devolverá tres posibles códigos (http):

- 200- Notificación do QR OK.
- 204- O idQR non existe / Erro.
- 502- Servizo QR caído

En fases posteriores, é previsible que na API analice todos os campos notificados polas expendedoras na chamada á API en tempo real para dar a notificación como válida. (Por exemplo , revisión do concello orixe/destino erróneo para o idQR notificado).

4.2. Notificación desde o backoffice da empresa de transporte

O proveedor de expendedoras debe notificar as validacións de QR que se realizaron nas expendedoras desde o seu backoffice (ou o backoffice subministrado polo proveedor de expendedoras á empresa de transporte) a XenteNova QR.

O obxectivo desta notificación é que XenteNova QR teña as validacións de QR por outro método alternativo ademais de en tempo real.

O backoffice das empresas de transporte realizará un agrupamento das validacións de QR da xornada por expendedora e liquidación (*json*) e enviaraas ao backoffice de XenteNova QR comprimidos en .zip.

Os parámetros a comunicar serán:





Cabeceira:

idFicheiro	string	idProvedor-IdMaquina+idliquidacion. Exemplo: 01-6580-AA0025
Data de xeración.	DateTime	Data na que se xerou a listaxe

Lista de obxecto validación QR

IdQr	int	Identificador único de cada código QR. Dato do QR
IdAccount	int	Identificador único de cada conta de usuario que utiliza o QR. Dato do QR.
IdProvider	int	Identificador do provedor de expendedoras desde o que se realiza a validación do QR. Neste campo ponse o identificador do provedor (GMV, Olton, Proconsi e IST) que está a notificar a validación do QR.
IsRealTime	boolean	Flag para indicar se a transacción é en tempo real, é dicir, se se está enviando esta transacción no momento no que se validou o QR. Provedores de expendedoras cubrir con True.
IdEquipment	int	Identificador do equipo que realiza a validación. Nº de serie expendedora.
TicketSerialNumber	String	Nº de serie do billete validado ou anulado. Ej. AA12345. Dato expendedora.
OperationDateTime	DateTime	Data e hora da validación/anulación/transbordo. Ej: 2022-09-01T15:09:29. Dato expendedora.
IdFare	int	Identificador da tarifa. N/A. Cubrir con 0.
Price	int	Prezo do billete equivalente TMG. Neste caso ten dous decimais implícitos no valor. Por exemplo, para 1,5 € represéntase en enteiro como 150, con dous decimais implícitos á dereita. Dato expendedora.
IdRoute	int	Identificador da liña de autobús onde se realizou a operación. Ide_Linea Sitme. Dato expendedora.





IdLine	int	Identificador do traxecto de autobús onde se realizou a operación. IdRutaSitme*10+Sentido. Dato expendedora.
IdExpedition	int	Identificador da expedición onde se realizou a operación. Id_Expedicion Sitme. Dato expendedora.
IdVehicle	string	Identificador do vehículo onde se realizou a operación (Matricula) Dato expendedora.
IdDriver	int	Codigo do condutor no que se realizou a operación. Dato expendedora.
IdOriginStop	int	Identificador da parada onde se realizou a operación. Id_paradaSitme. Dato expendedora.
IdOrigin	int	Identificador da orixe, que non é parada, onde se realizou a operación. Neste caso trátase do identificador do Sitme do concello orixe. Dato expendedora.
IdDestinationStop	int	Identificador da parada destino, que sería a última parada do traxecto onde se realizou a operación. IdparadaSitme. Dato expendedora.
IdDestination	int	Identificador do destino. Neste caso trátase do identificador do Sitme do concello destino. Dato expendedora.
OperationType	int	Identificador do tipo de operación. 1 – Validación de QR 25 – Anulación de validación 100 – Erro Dato expendedora.
OperationResult	int	Identificador do resultado da operación. 0 – Validación OK 1 – QR caducado 2 – QR Passback 3 – QR erro Orixe-Destino 4 – QR erro formato Dato expendedora.
Signature	String	Sinatura do QR. É un valor de 128 bytes, polo que se pasa como String representando a cadea de bytes en hexadecimal. Dato QR





Exemplo do contido do ficheiro listado de validacións de QR

```
{
  "idFicheiro": "01-6555-AA0025",
  "dataXeración": "2022-09-01T15:09:29",
  [
    {
      "idQr": 28,
      "idAccount": 1,
      "idProvider": 1,
      "isRealTime": false,
      "idEquipment": 6555,
      "ticketSerialNumber": "string",
      "operationDateTime": "2022-09-01T15:09:29",
      "idFare": 0,
      "price": 88,
      "idRoute": 1524,
      "idLine": 11,
      "idExpedition": 99584,
      "idVehicle": "1255LDB",
      "idDriver": 1,
      "idOriginStop": 257,
      "idOrigin": 1,
      "idDestinationStop": 38764,
      "idDestination": 108,
      "operationType": 1,
      "operationResult": 0,
      "signature":
        "1CEC8A9C9752D10A72D55EC2A3A8B5E414AAE2ED6597964E77251DC2176
        4BC35EBBC6C97FD2F2BFC515564D9A4AA76BC54AFE0C64091881027F8E17
        CFD580945E5475259CE2F57CD668A12D856FC25C05C8EED96DÁ3F03FEC4
        9C591B670075F3327CA13F33ED00289F2518406E20E25E8027C1FC5CAB6B8
        A3A7CA 7ECB298503E"
    }
  ]
}
```





```
"operationDateTime": "2022-09-01T15:19:29",
"idFare": 0,
"price": 88,
"idRoute": 1524,
"idLine": 11,
"idExpedition": 99584,
"idVehicle": "1255LDB",
"idDriver": 1,
"idOriginStop": 257,
"idOrigin": 1,
"idDestinationStop": 38764,
"idDestination": 108,
"operationType": 1,
"operationResult": 0,
"signature":
"1CEC8A9C9752D10A72D55EC2A3A8B5E414AAE2ED6597964E77251DC21764BC35E
BBC6C97FD2F2BFC515564D9A4AA76BC54AFE0C64091881027F8E17CFD580945E5
475259CE2F57CD668A12D856FC25C05C8EED96DÁ3F03FEC49C591B670075F3327
CA13F33ED00289F2518406E20E25E8027C1FC5CAB6B8A3A7CA7ECB298503E"
}
]
}
```

4.2.1. Respostas da API á notificación dunha validación

Á súa vez XenteNova QR proverá un *webservice* para coñecer o estado de cada ficheiro remitido desde o *backoffice* das empresas de transporte.

5. Notificación das operacións a Sitme .

O provedor de expendedoras debe notificar todas as operacións ao Sitme, é dicir hanse de enviar as operacións a través dos ficheiros de colectas definidos polo Sitme.

Deste xeito, o sistema QR XenteNova conta cun sistema de información das operacións en tempo real (notificacións á API) e outro offline a partir da notificación de operacións de cada provedor ao Sitme. Hase de axustar /modificar por tanto o envío de colectas por parte dos provedores de expendedoras ao novo formato de colectas que indique o Sitme.





6. Comprobacións a realizar na expendedora

6.1. Proceso de autenticación

6.1.1. Comprobación de lonxitude e decodificación base64

O primeiro paso, como se mencionou previamente, é comprobar que a lonxitude e o contido do QR son correctos. Se o son, procédese a decodificar o base64, obtendo o seguinte:

BASE64:

```
AAEAAACPAAAAAwEAAABsAAABBB1yiAABco277AAEAtAABF9m07ZMhkkETmliDtn9  
nhyFA6kIILp3D2ZKqg4QZ4ZEa8yxQVJhmuTKnK8Gy6JchwsqCvdn7vCD7x4gDbNve  
KT/wq7E4RbWSCZ+vEe9g2lwtXXOBTUpr3WSxiDtDst1kt8z8TXCvui+KDnQUAYV/Kof  
7N7ELmTYdczE0dvW6NdU2KXGXlUmzRQ==
```

HEX:

```
00010000008F00000003010000006C000001075CA200005CA36EFB000100B400  
0117D9B4ED9321924113988883B67F67872140EA42252E9DC3D992AA838419E1911A  
F32C50549866B932A72BC1B2E89721C2CA82BDD9FBBC20FBC788036CD55E293FF0  
ABB13845B592099FAF11EF60DÁ5C2D5D7381B54A6BDD64B1883B43B2DD64B7CCF  
C4D70AFBA2F8A0E741403257F2A87FB37B10B99361D73313476F5BA35D536297197  
9549B345
```

Morado = Parte estática do QR (33 bytes).

Azul = Parte de autenticación do QR (128 bytes).

Verde = Parte dinámica do QR (8 bytes).

Como exemplo, proporciónase o seguinte código sobre a decodificación de base64 en C++ (función base64_decode): <https://github.com/arrowhead-f/clientcpp/blob/master/ConsumerExample/src/Security/base64.cpp>.

6.1.2. Comprobación de sinatura

A expendedora contará con 10 claves para comprobar a parte autenticación. Cada clave está contida nun ficheiro con extensión PEM, que á súa vez contén unha cadea de texto co seguinte formato (primeira clave):

```
-----BEGIN PUBLIC KEY-----
```





```

MIGeMA0GCSqGSib3DQEBAQUAA4GMADCBiAKBgF7Qu36bTZzyGnLZcHsv
NQgPt/NDvNkdFhEmKi4FqddsT1p9tCKjJRTTrFu3ZTmR+w7brnOiTBxY9E3Nu
Dq0E3SKREhkVKWHwRQs0qMQDtOo3+m3iC+QLOdfKdJd+SGTUqBayfouW
FpYzetArKgBxwK2STUY6
/Yc0p5cFQiX4Gdc3AgMBAAE=
-----END PUBLIC KEY-----

```

O equipo de soporte do proxecto na AMTEGA subministrará o ficheiro PEM a cada provedor.

O campo do QR **ID clave sinatura** indica cal das 10 claves hai que usar (é dicir, cal dos 10 ficheiros PEM). Asumindo o QR posto de exemplo, é a primeira clave e, a nivel ilustrativo, achégase o seguinte exemplo en pseudocódigo C++ usando a librería OPENSSL. Como nota, *publicKey* debe apuntar á primeira posición do ficheiro PEM en cuestión, é dicir, le directamente o ficheiro desde o principio:

```

#include <openssl/ssl.h>

#define XA256_HASH_LEN 32
#define RSA_SIGNATURE_MAX_LEN 256
bool RSAVerifySignature( const char* publicKey, size_t publicKey_len, const
char* staticpart, size_t staticpart_len, const char* signature, size_t
signature_len, bool* authentic)
{
    bool ret = true;
    unsigned char decrypted_data[RSA_SIGNATURE_MAX_LEN];
    unsigned char hash[XA256_HASH_LEN];

    *authentic = false;

    if(signature_len > RSA_SIGNATURE_MAX_LEN)
    {
        ret = false;
        //RSA ERRO: signature size not supported
    }

    if(ret == true)
    {
        ret = false;

        BIO *keybio = BIO_new_mem_buf((void*)publicKey, publicKey_len);
        if(keybio!=NULL)
        {

```





```
RSA *rsa = PEM_read_bio_RSA_PUBKEY(keybio, &rsa, NULL, NULL);

if(rsa!=NULL)
{
    int decrypted_len = RSA_public_decrypt(signature_len,(const
unsigned char*)signature,decrypted_data,rsa,RSA_PKCS1_PADDING);
    if(decrypted_len < 0)
    {
        //RSA_public_decrypt ERROR
    }
    else
    {
        {
            ret = true;
        }
    }
    else
    {
        //RSA ERROR
    }
}
else
{
    //BIO_new_mem_buf ERROR
}
}

if(ret == true)
{
    SHA256_CTX sha256;
    SHA256_Init(&sha256);
    SHA256_Update(&sha256,staticpart,staticpart_len);
    SHA256_Final(hash, &sha256);

    if(!memcmp(hash,&decrypted_data[19],sizeof(hash)))
    {
        //¡Sinatura autentica!
        *authentic = true;
    }
}

return ret;
}
```



Finalmente comparar hash con respecto aos datos descriptados, faise con respecto ao índice 19 polo sistema de encriptado empregado, ilustrativamente:

- *decrypted_data* (hex):
3031300D060960864801650304020105000420**6BF76CC66086EBE342141B13A7245ED79BC5CA4DÁ2EA2DF8B21D8175732 F4CF6**.
- *hash* (hex):
6BF76CC66086EBE342141B13A7245ED79BC5CA4DÁ2EA2DF8B21D8175732 F4CF6.

Por suposto, existe liberdade á hora de elixir a implementación para a comprobación da sinatura.

6.1.3. Decodificación de data-hora de xeración / refresco

Esta data-hora atópase encriptada usando TDES CBC con vector de inicialización 0 e como clave os 8 primeiros bytes da clave pública do QR en cuestión.

Para o exemplo que nos ocupa, data-hora é en *hex* 362971979549B345 e os 8 primeiros bytes da clave (que previamente se decodificou de base64) son, en *hex*, 30819E300D06092A. Esta descriptación pódese facer usando a librería DES de OPENSLL (xa usada previamente para a sinatura) ou calquera outra implementación (como exemplo, <https://github.com/ruCyberPoison/oscam-r11429/blob/master/cscrypt/deas.c>).

O resultado é, en *hex*, **5CA2C1C5**00000000, dos que só son relevantes os 4 bytes de maior peso. Por tanto, o número *hex* 5CA2C1C5 corresponde, co formato data-hora, ao seguinte: 17/02/23 12:07:05.

6.2. Proceso de autenticación

O proceso de autenticación consta de tres partes: verificar que a lonxitude do QR é correcta, que o seu contido está en formato base64 e, logo da súa decodificación, comprobar coa sinatura que é un QR válido.

6.3. Proceso de validación

O proceso de validación ten os seguintes pasos, calquera sentenza supón erro na validación:

1. Comprobar que o saldo é maior que 0.
2. Comprobar que coincide a orixe e destino co actual da expendedora.
3. Comprobar que a data-hora de uso do QR é válida.
4. Comprobar que a data-hora dinámica de uso do QR é válida.
5. Comprobar que o identificador QR non está na lista negra local (da expendedora).





6.3.1. Comprobación de data-hora dinámica de uso do QR é válida

Compárase data+hora da expendedora para verificar que este dentro do rango con data+hora de refresco $\pm$ a validez dinámica entre dous.

Exemplo:

Data +hora da expendedora: 15:01:25

Data +hora de refresco do QR (parte dinámica) -> 15:01:18

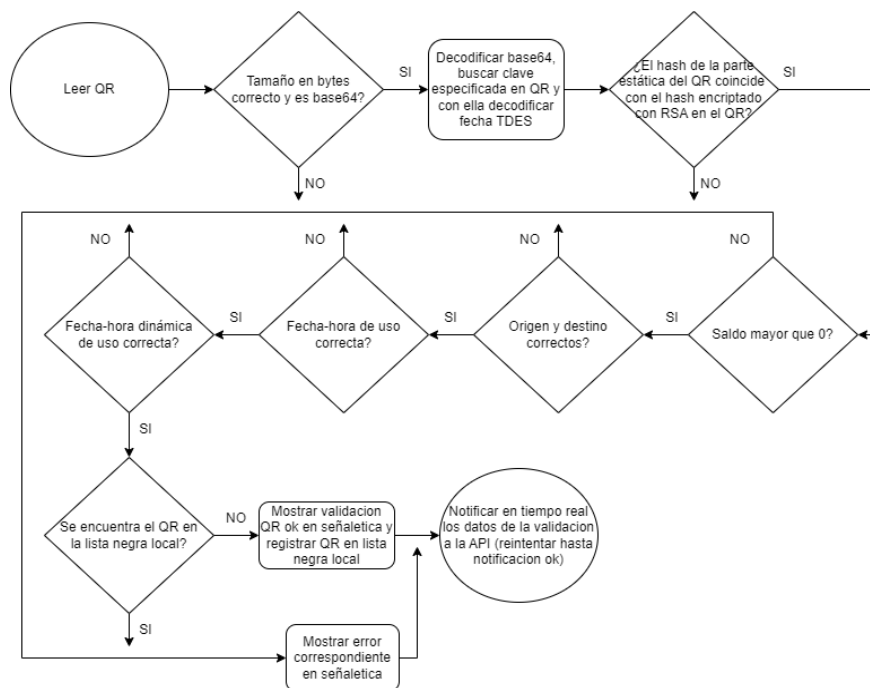
Validez dinámica do QR -> 91 segundos (dividir entre dous e se impar redondear á alza)

O QR é válido no rango:

$15:01:18 - 46 = 15:00:32$

$15:01:18 + 46 = 15:02:04$

6.4. Diagrama do proceso de autenticación e validación



6.5. Lista negra local na expendedora



A expendedora gardará nun ficheiro local o campo "Identificador conta" de todos os QR que se validen satisfactoriamente para asegurarse de que non se validan de novo durante a expedición.

Evítase así que unha persoa usuaria poida validar na mesma expedición dous QRs de forma seguida. Lembremos que coa tarxeta XenteNova física a persoa usuaria pode validar dúas veces seguidas pero a administración só lle abona a primeira das viaxes.

Logo de pechar a expedición pódese borrar a lista negra da expendedora.

6.6. Proceso de anulación

- **FASE1**

A persoa usuaria poderá solicitar ao/á condutor/a a anulación de, cando menos, a última validación realizada con QR. Para iso a persoa usuaria indicará ao/á condutor/a o número de serie do billete a anular e este/a último/a procederá a anular a validación na expendedora. Entregáveselle á persoa usuaria un ticket de anulación (mesmo procedemento que a anulación dun billete en efectivo). En tempo real envíase a notificación da anulación á API XenteNova para actualizar os datos da conta da persoa usuaria. En paralelo, gardárase a operación para notificar a anulación a través do *backoffice* da empresa de transporte e das colectas.

- **FASE2**

Prevese a futuro que a APP poida presentar un QR xa validado á expendedora para tramitar a súa anulación.

7. Información ás persoas usuarias

7.1. Sinalítica a bordo

A expendedora debe comportarse como unha validación de tarxeta TMG (asubío de validación OK ou erro, luz verde indicando que a validación foi correcta, etc.).

7.2. Ticket ao usuario

Subministrárase á persoa usuaria un ticket co mesmo formato que a validación da tarxeta TMG, coa excepción de que non se indicará o prezo no ticket ou, no seu defecto, indicárase 0€.

Nótese que, na notificación á API, remitírase o importe do billete TMG equivalente.

Subministrárase á persoa usuaria un ticket de anulación, logo da súa solicitude dunha anulación de QR.





A impresión do ticket logo dunha validación/anulación de QR na expendedora será configurable, xa que se prevé a futuro que se poida xerar un ticket virtual na APP, momento no cal se solicitará que se deshabilite a entrega de ticket por parte da expendedora.

8. Probas con APP (iOS e Android) e homologación.

Para poder realizar probas de funcionamento, o equipo de soporte do proxecto na AMTEGA, subministrará ao proveedor de expendedoras a APP que xera QRs contra a contorna de pre-producción da AMTEGA. Deste xeito, a empresa provedora de expendedoras poderá xerar QRs para verificar a correcta implementación dos desenvolvementos.

Previo á fase de pilotos, haberá unha fase de homologación polo equipo de soporte do proxecto na AMTEGA para a comprobación do correcto funcionamento dos desenvolvementos.



ANEXO II

Formato de Colectas v.6

1. Descrición ficheiro de colecta V6.0

A colecta é un ficheiro ASCII de lonxitude de rexistro variable. O identificador de remate de rexistro é o carácter *Retorno de carro Windows* (delimitador OD OA). Nesta versión de ficheiro de colecta non se enche a espazos ata conseguir un tamaño fixo de rexistro co obxectivo de diminuír o tamaño de ficheiro.

O nome do ficheiro é "oooppnnnnn.lib", sendo "ooo" o código identificador de operador (OT), "pp" o identificador do provedor do OT (por se existisen dous provedores para un OT), e "nnnnn" un contador secuencial de colectas enviadas polo operador (continúase o contador actual).

Presenta 6 tipos de rexistro, que deberán ser enviados de forma ordenada no ficheiro:

1. Cabeceira ("00"). Contén o identificador do ficheiro e datos xerais do mesmo. Existe un único rexistro "00" por ficheiro de colecta.
2. Viaxes ("01"). Recolle a oferta realizada polo operador. Existen múltiples rexistros "01" por ficheiro de colecta.
3. Billetes non Financeiros ("02"). Información dos billetes abonados cun medio de pagamento distinto á tarxeta metropolitana (efectivo e bonos, entre outros). Existen múltiples rexistros "02" por ficheiro de colecta. Os rexistros débense ordenar por "número de viaxe".
4. Billetes Financeiros ("03"). Billetes abonados coa tarxeta metropolitana ou compatible (p.e. tarxeta de Tranvías da Coruña). O rexistro "03" contén información adicional á de Billetes non Financeiros (é dicir, poderíase considerar que a estrutura dos Billetes é única, coa particularidade de que os Billetes non Financeiros non teñen os campos finais e presentan un ide rexistro distinto). Existen múltiples rexistros "03" por ficheiro de colecta. Os rexistros débense ordenar por "número de viaxe".
5. Billetes QR ("05"). Información dos billetes abonados mediante pagamento por QR desde aplicación móbil ou similar. Existen múltiples rexistros "05" por ficheiro de colecta. Os rexistros débense ordenar por "número de viaxe".





6. Billetes Financeiros con erro ("04"): Billetes abonados con tarxeta metropolitana ou compatible incompletas, debido a algún tipo de erro (estado<>'00'). Estes rexistros unicamente conterán os campos de información dispoñibles. Existe ningún ou varios rexistros "04" por ficheiro de colecta. Os rexistros débense ordenar por "número de viaxe".
7. Totais ("09"). Campos de control que totalizan rexistros e importes. Existe un único rexistro "00" por ficheiro de colecta.

Os campos numéricos encheranse a ceros pola esquerda ata completar a lonxitude definida (número de caracteres ascii). Os campos alfanuméricos completaranse con espazos pola dereita. Terminoloxía:

- Anulación: billete anulado a bordo. Na colecta existirán dous rexistros, o da venda, e o da anulación. Han de figurar de forma consecutiva na colecta.
- Eliminación: proceso extraordinario para eliminar un billete (polo momento só se utilizará para o billete financeiro) que contén un erro non emendable, e que provocou previamente un rexeitamento da colecta. A colecta rexenerouse e reenviouse, eliminando (eliminación lóxica, non física) os billetes con erros non emendables.

2. Cabeceira

Nome	TIPO	POS	LON G	Descrición
Id rexistro	N	1	2	"00": cabeceira
Id empresa	N	3	3	Identificador da empresa
Número de colecta	N	6	7	Contador de ficheiro enviado pola empresa(acumulado total, non diario)
Data crea	N	13	8	AAAAMMDD
Hora crea	N	21	6	HHMMSS
CIF	A	27	9	CIF da empresa
Nome empresa	A	36	30	Nome empresa
Número de envío	N	66	2	Número de envío da colecta
Versión de colecta	N	68	3	Versión de estrutura colecta (esta é a `006`)
Versión de mestres.	N	71	5	Versión de mestres.





3. Viaxes

Nome	TIPO	POS	LONG	Descrición
Ide rexistro	N	1	2	"01": viaxes
Número de rexistro.	N	3	6	Secuencial de rexistro de Viaxes, comezando en "000001"
Id Expendedora	N	9	8	Identificador da expendedora
Número viaxe	N	17	8	Secuencial de viaxe da empresa.
Id Liña	N	25	5	Identificador da liña
Id Expedición	N	30	8	Identificador da expedición
Vehículo	N	38	10	Identificador do vehículo
Condutor	N	48	8	Identificador do condutor
Data de Saída.	N	56	8	Data de saída da viaxe AAAAMMDD
Hora de Saída.	N	64	6	Hora de saída da viaxe HHMMSS
Data de Chegada.	N	70	8	Data de chegada da viaxe AAAAMMDD
Hora de Chegada.	N	78	6	Hora de chegada da viaxe HHMMSS
Parada Orixe	N	84	5	Parada orixe da viaxe
GPS N PO	N	89	10	Pos GPS Norte Parada de Orixe en formato WGS84 sen punto: GGGMMmmmm
GPS W PO	N	99	10	Pos GPS Oeste Parada de Orixe
Manual/Aut PO	N	109	2	Obtención do valor de Parada de Orixe (00 GPS, 01 Manual)
Parada Destino	N	111	5	Parada destino da viaxe
GPS N PD	N	116	10	Pos GPS Norte Parada de Destino (formato WGS84 GGGMMmmmm sen punto, sendo m os decimais dos Minutos M).
GPS W PD	N	126	10	Pos GPS Oeste Parada de Destino





Nome	TIPO	POS	LONG	Descrición
Manual/Aut PO	N	136	2	Obtención do valor de Parada de Destino (00 GPS, 01 Manual)
Viaxeiros	N	138	5	Número de viaxeiros non anulados
Viaxeiros nulos	N	143	5	Número de viaxeiros anulados
Recadación efectivo	N	148	8	Recadación efectivo en céntimos de euros non anulado. Non se contabiliza a paquetería.
Recadación Tarxeta Metropolitana	N	156	8	Recadación Tarxeta Galicia en céntimos de euros non anulado. Non se contabiliza a paquetería.
Cantidade pendente subvención	N	164	8	Recadación pendente de subvención en milésimas de euros non anulado
Recadación outros medios de pagamento	N	172	8	Recadación outros medios de pagamento en céntimos de euros non anulado. Non se contabiliza a paquetería.
Indicador de viaxe eliminada	N	180	1	Viaxe eliminada S/N
Tipo de Venda	N	181	2	Tipo de venda ("01" Vehículo; "02" Despacho de billetes; "03" Expendedora Automática; "04" Manual; "05" Internet; "06" GPRS)





4. Billetes non financeiros

Id de rexistro=02. Os primeiros 24 campos (sombreados) son comúns a ambos os tipos de billetes. (financeiros e non financeiros). Os restantes son informacións unicamente dos Billetes Financeiros (non existirán nos Billetes non Financeiros).

Nos billetes non financeiros enviaranse 111 posicións. Non é necesario manter un ancho de rexistro fixo en todo o ficheiro enchendo a espazos.

5. Billetes financeiros

Envíanse indistintamente (sen orde especial entre elas) en rexistros "03" as operacións de tarxetas con contactos e as dobre interface. Co obxectivo de causar menos impacto, déixanse inalterados os campos actuais da TMG con contactos e engádense ao final os novos campos necesarios para a TMG dual.

As operacións de tarxetas con contactos non encherán os 9 últimos campos, engadidos para a TMG dual (en cursiva). Enviaranse 211 posicións por rexistro para este tipo de operacións. NON é necesario manter un ancho de rexistro fixo, e así se consegue un menor tamaño de ficheiro.

As operacións de tarxetas dobre interface utilizarán os últimos 9 campos (en cursiva), e recherán a espazos os campos en cor vermella, que son aqueles que están duplicados por estar contemplados dentro das últimos 9 estruturas de información. O último campo (evento máis recente) só é necesario escribilo cando o último evento (que é o que devolve a tarxeta no OpenValidatorSession) non é un consumo ou transbordo. Enviaranse 393 posicións cando o último evento sexa consumo ou transbordo, e 451 cando este sexa doutro tipo (anulación consumo, anulación carga, ou regularización).

NOMBRE	TIPO	POS	LONG	DESCRIPCIÓN
Id rexistro	N	1	2	"02": billetes non financeiros "03": billetes financeiros "04": billetes financeiros con erro (estado<>'00') "05": billetes con QR Xente Nova
Número de rexistro.	N	3	6	Secuencial de rexistro de Billetes non financeiros, ou secuencial de Billetes Financeiros, ou secuencial de billetes con QR Xente Nova, comezando sempre en "000001".





NOMBRE	TIPO	POS	LONG	DESCRIPCIÓN
Id Expendedora	N	9	8	Identificador da expendedora
Número viaxe	N	17	8	Secuencial de viaxe da empresa
Número	N	25	5	Identificador da venda de cada máquina (para Facenda). Numéranse unicamente as vendas. As anulacións incorporan a numeración do billete anulado.
Serie	A	30	2	
Data de Venda	N	32	8	Data de venda AAAAMMDD
Hora de Venda	N	40	6	Hora de venda HHMMSS
Tipo de operación	N	46	2	Tipo de operación ("00" venda; "10" anulación venda "01" venda paquetería; "11" anulación paquetería)
Viaxeiros	N	48	2	Número de viaxeiros da venda (multiviaxe)
Liña	N	50	5	Identificador da liña
Parada Orixe	N	55	5	Identificador de parada orixe
GPS N PO	N	60	10	Pos GPS Norte Parada de Orixe (formato WGS84 GGGMMmmmm sen punto, sendo m os decimais dos Minutos M).
GPS W PO	N	70	10	Pos GPS Oeste Parada de Destino
Manual/Aut PO	N	80	2	Obtención do valor de Parada de Orixe (00 GPS, 01 Manual)
Parada Destino	N	82	5	Identificador de parada destino
Tarifa Especial	N	87	5	Identificador de tarifa especial.
Perfil de operación	N	92	3	Perfil aplicado á operación (coincide co perfil de desconto da tarxeta se se aplica o desconto especial, e se non perfil normal "001").
Id Medio de pagamento	N	95	2	"01": TMG ou tarxeta compatible (p.e. tj de Tranvías da Coruña); "02": efectivo; "03": outros (bonos, tarxetas propietarias non compatibles); "05": QR XenteNova
Importe	N	97	5	Importe da venda ou anulación sen decimais (en céntimos de euro)
Divisa	N	102	3	Divisa do importe ("978" para euros)





NOMBRE	TIPO	POS	LONG	DESCRIPCIÓN
Indicador Tarifa Única	B	105	1	Indicador de Tarifa Única (S/n)
Indicador de Billete eliminado	B	106	1	Billete eliminado S/n (elimínase de forma lóxica, non física, un billete cando se reenvía unha colecta fora rexeitada por conter datos de operación financeira inválidos).
Subvención prevista	N	107	5	Subvención prevista en milésimas de euro
Id Tarxeta	N	112	16	Número de tarxeta PAN
Contador social	N	128	4	Número de viaxes do contador social INICIAL
Data caducidade contador	N	132	8	Data de caducidade do contador AAAAMMDD
Indicador transbordo aplicado	N	140	1	Indicador de aplicación do transbordo. "0": non; "1": si
Id concello anterior	N	141	5	Concello orixe da operación anterior lido da tx. [utilizado nas operacións de tx dual cando exista transbordo, para o último evento lido de tipo consumo ou transbordo, que serve para a aplicación do transbordo]
Id liña anterior	N	146	5	Liña anterior lido da tarxeta [utilizado nas operacións de tx dual cando exista transbordo, para o último evento lido de tipo consumo ou transbordo, que serve para a aplicación do transbordo]
Data Anterior	N	151	8	AAAAMMDD lido da tarxeta [utilizado nas operacións de tx dual cando exista transbordo, para o último evento lido de tipo consumo ou transbordo, que serve para a aplicación do transbordo]
Hora Anterior	N	159	4	HHMM lido da tarxeta [utilizado nas operacións de tx dual cando exista transbordo, para o último evento lido de tipo consumo ou transbordo, que serve para a aplicación do transbordo]
PSAM_CAN	N	163	8	PSAM da canceladora (do EFsam na tarxeta dobre interface)
Estado	N	171	2	Estado da operación na tarxeta. "00": OK <>"00" erro, segundo lista.
Asina tarxeta	A	173	16	Sinatura de consumo S3 realizada pola tarxeta con contactos / MAC de operación da tarxeta dual





NOMBRE	TIPO	POS	LONG	DESCRIPCIÓN
NT	N	189	5	Número de transacción da tarxeta
NTPSAM	N	194	10	Contador de transaccións da canceladora (a ceros en tarxeta dobre interface)
Saldo	N	204	8	Saldo final da tarxeta
VALCHALLENGE	A	212	8	Número xerado polo terminal, 4 bytes hexa.
ULTIMO EVENTO	A	220	58	Evento anterior enviado na sesión, 29 bytes hexa. Devolto pola tarxeta no OpenValidatorSession. A partir deste campo, incluído, son os 7 campos de información que se envían ao módulo SAM para certificar os datos.
ESTRUTURA DE CONTORNA	A	278	18	Estrutura de contorna da tarxeta 9 bytes hexa
ESTRUTURA DE USUARIO	A	296	24	Estrutura de usuario da tarxeta 12 bytes hexa
CONTADOR DE UNIDADES DO FICHEIRO DE BALANCE	A	320	6	Saldo do ficheiro balance que non se usa. Non se xestiona o seu contido, pero débese incluír o mesmo valor que devolve a tarxeta no OpenValidatorSession e que se envía ao SAM, porque se asina
RATIFICACION	A	326	2	Byte de ratificación. Non se xestiona o seu contido, pero débese incluír o mesmo valor que se enviou ao SAM, porque se asina.
CARDCHALLENGE	A	328	8	Número xerado pola tarxeta. 4 bytes hexa.
NOVO EVENTO A ESCRIBIR	A	336	58	Evento a gravado na tarxeta. 29 bytes hexa.
EVENTO MÁIS RECENTE DE CONSUMO	A	394	58	Evento máis recente que é un consumo ou transbordo lido da tarxeta. Só se ha de escribir este campo cando o último evento que devolve a tarxeta no OpenValidatorSession non é consumo ou transbordo.
TOTAL:		451 posicións		





ESTRUTURA DE CONTORNA

A estrutura de contorna emprégase para almacenar información xeral relativa á propia aplicación de transporte.

Bits	Nome	Pos. Bitmap	Contido	Tamaño (bits)
1..6	Versión da Aplicación		000001	6 bits
7..12	Mapa de bits xeral (*)		110000	6 bits
13..36	Contorna de Rede de traballo.	[0]	987000h	24 bits
37..44	Contorna de aplicación	[1]	02h (TMG); 01h (Conc A Coruña)	8 bits
45..58	Data de caducidade da aplicación	[2]	Non utilizada	14 bits
59..69	Método de Pagamento	[3]	Non utilizada	11 bits
	Sinatura de contorna	[4]	Non utilizada	
	Datos de contorna	[5]	Non utilizada	
	RFU (Reservado Futuros Usos)		Non utilizada	

(*) Nota: Un bit a cero significa que o campo non está presente na estrutura.

ESTRUTURA DE USUARIO/A

A estrutura de usuario/a utilízase para almacenar información xeral do/a usuario/a da tarxeta, e o perfil de comportamento.

BYTES	Nome	Contido	Tamaño
1	Perfil de desconto.	Perfil de usuario ou perfil social. Determina o tipo de desconto a aplicar nun traxecto. O Perfil de desconto "01h" é o perfil normal. As tarxetas compatibles coa TMG deben acordar os perfís de desconto coa DXT.	1 byte
2..3	Data de inicio do perfil	Formato Data (ver anexo): Se valor cero, non se avalía o seu contido.	2 bytes
4..5	Data de caducidade do perfil	Formato Data (ver anexo): Se valor cero, non se avalía o seu contido.	2 bytes
6..7,5	Concello emisor	Código de Concello emisor. Non se xestiona o seu contido.	1,5 bytes
7,5..8,5	Código de colectivo	Código de colectivo social. Non se xestiona o seu contido	1 byte
8,5..12	RFU (Reservado Futuros Usos)	Non se xestiona o seu contido	36 bits





ESTRUTURA DE EVENTOS

POS	Nome	Contenido	Tamaño
1-2	NT tarxeta [NT]	Número de transacción do ficheiro de eventos	2 bytes
3-4	Importe [ImpEvent]	Importe en hexadecimal. Correspóndese co DecValue a enviar no CloseValidatorSession	2 bytes
5-7	Saldo anterior [BalEvent]	Saldo en hexadecimal.	3 bytes
8	Tipo de transacción [TransEvent]	01b: consumo; 00b: anulación de consumo	2 bits
	RFU	Non utilizado	1 bit
	Contrato	Nº de contrato (00001b)	5 bits
9	Versión estrutura de evento	Versión de estrutura (0001b)	4 bits
	Sentido da viaxe	0, ida (sentido crecente na ordenación de paradas da liña nos datos mestres); 1, volta	1 bit
	Clase de transacción	000b transbordo (se se aplica desconto por transbordo, total ou parcial) 001b consumo (cando sexa un consumo sen desconto por transbordo) 010b regularización C.V.bonificados 011b anulación de carga	3 bits
10	Operador	Código de operador en hexadecimal.	1 byte
11	Perfil de operación	Perfil da operación. Coincide co perfil de desconto da estrutura de usuario se se aplican descontos especiais sociais. Se se aplica o perfil normal: 01h	4 bits
12-13	Liña	Código de liña en hexadecimal.	2 byte
14-15	ContadorVendas / Oficina	ContadorVendas ¹ / oficina (en anulación carga) / terminal (en regularización) en hexadecimal.	2 bytes

¹ **contador vendas**: Cada expendedora debe levar un contador de vendas para todos os medios de pagamento (campos **Número** e **Serie** da Colecta). Neste campo da tarxeta (**Contador Vendas**) débese gravar o campo **Número** da colecta, de tal forma que ambos coincidan nas vendas de tarxeta. Este campo non debe presentar duplicacións nin saltos de numeración. Reiniciárase o contador da expendedora ao alcanzar o límite. O límite será 65.535 (2 bytes), aínda que tamén se acepta un límite inferior por cuestións prácticas existentes.





POS	Nome	Contenido	Tamaño
16-17	Data de transacción	Formato(*) data en 2 bytes	2 bytes
18-19	Hora e minuto da transacción	HHMM en BCD	2 bytes
20-21	Número de viaxeiros.	Número de viaxeiros da multivenda en hexadecimal.	4 bits
	Contador viaxes bonificadas realizados	Contador crecente do número de viaxes sociais realizadas. Non se incrementa se se aplica o perfil normal. En hexadecimal.	12 bits
22	Divisa do saldo	11 euros; 01 viaxes	2 bits
	Tarifa única	Indicador de Tarifa Única (1: Si, 0: non)	1 bit
	Area Metropolitana	Código de AM en hexadecimal (1: Ferrol; 2:Coruña; 3:Santiago)	5 bits
23-24	Parada orixe	Código de parada orixe en hexadecimal.	2 bytes
25-26	Parada destino	Código de parada destino en hexadecimal.	2 bytes
27-29	Concello Orix	Código de Concello Orix en hexadecimal.	1,5 bytes
	Concello Destino	Código de Concello Destino en hexadecimal.	1,5 bytes
30	Bit de Ratificación	Non se xestiona o seu contido	1 byte
31-32	RFU		2 bytes

Os campos sombreados son xestionados polo Sistema Operativo.

A estrutura desde o byte 9 ao 29 ambos os incluídos (21 bytes) denomínase [EventStruct] na documentación descritiva do Sistema Operativo MMAR CEN/WG10 – dual interfase v4.1 – especificación funcional.

Sempre se utilizan os 29 primeiros bytes de forma consecutiva:
NT+ImpEvent+BalEvent+TransEvent+EventStruct.

Codificación dos erros na operación de tarxeta (valores do campo "Estado"):

ERRO	DESCRCIÓN
1	Tarxeta non responde
2	Lectura de ficheiro EF_CARD
3	Selección de aplicación
4	Lectura de IEP
5	Lectura ficheiro de saldo
6	Lectura ficheiro administrativo
7	Gravación ficheiro administrativo





ERRO	DESCRICIÓN
8	Inicialización do IEP para compra
9	Sinatura S1 errónea
10	Comprobación de saldo
11	PSAM incorrecto
12	Lectura de histórico
50	Divisa incorrecta
51	Tarxeta persoal
52	Perfil non válido
53	Saldo insuficiente
60	ANULACION: Tarxeta non coincide
61	ANULACION: Rexistro non coincide
62	ANULACION: PSAM non coincide



6. Billetes QR

Id de rexistro =05. Os primeiros 24 campos (sombreados no apartado de billetes financeiros) son comúns ao resto de tipos de billetes. (financeiros, non financeiros e QR.

A maiores dos 24 primeiros campos, engadiranse

NOME	TIPO	POS	LONG	DESCRIPCIÓN
IdQr	N	112	10	Identificador único do QR, ej:1234567891
IdCuenta	N	122	10	Identificador único da conta, ej:1234567891
Sinatura do QR	A	132	256	Sinatura xerada con RSA
IdProveedor Validadora	N	388	2	Identifica o proveedor da validadora onde se realizou a venda/anulación/erro: Ej: 1: Olton, 3:GMV, 5:Proconsi, 7:IST
idExpedicion	N	390	10	IdSitme expedición na que se realizo a validación/anulación/erro Ej: 12152
idConcelloOrixe	N	400	5	IdSitme do concello orixe onde se realizo a validación/anulación/erro
idConcelloDestino	N	405	5	IdSitme do concello destino onde se realizo a validación/anulación/erro
Resultado Operación QR	N	407	2	Identifica o resultado da validación no vehículo: • 0 - Validación OK • 1 - Erro en validación: Data validez do QR errónea • 2 - Erro en validación: Concello orixe do QR erróneo • 3 - Erro en validación: Concello destino do QR erróneo • 4 - Erro en validación: Sinatura do QR errónea





7. Totais

Para os totais de rexistros contaránse todos eles, tanto vendas como anulacións.

Para os totais de importes sumaranse as vendas e restaranse as anulacións (ou sumar todos se se consideran os importes anulados negativos).

Os billetes eliminados (cando se pon a 1 o indicador de billete eliminado, para corrixir unha colecta rexeitada) deben ser descontados nos importes.

Para os totais si se conta a paquetería.

NOME	TIPO	POS	LONG	DESCRICIÓN
Id rexistro	N	1	2	"09": totais
Número de rexistros total	N	3	7	Número de rexistros total do ficheiro, incluíndo cabeceira e totais, e todo tipo de rexistros
Número de rexistros de Viaxes ('01')	N	10	7	Número total de rexistros de Viaxes.
Número de rexistros. Billetes non Financ. ('02')	N	17	7	Número total de rexistros de Billetes non Financeiros
Número de rexistros Billetes Financ. ('03')	N	24	7	Número total de rexistros de Billetes Financeiros ou tarxeta metropolitana.
Importe Billetes non Financ.	N	31	9	Suma do campo Importe dos Billetes non Financ.
Importe Billetes Financ.	N	40	9	Suma do campo Importe dos Billetes Financ. ou TMG
Importe subvencionado	N	49	9	Suma do campo <i>subvención prevista</i> de todos os Billetes, en milésimas de euro.
Número de rexistros de Viaxes eliminadas	N	58	7	Número de rexistros de Viaxes eliminadas
Número de rexistros Billetes non Financeiros eliminados	N	65	7	Número de rexistros de Billetes non Financeiros eliminados
Número de rexistros Billetes Financeiros eliminados	N	72	7	Número de rexistros de Billetes Financeiros eliminados





NOME	TIPO	POS	LONG	DESCRICIÓN
Importe Billetes non Financeiros eliminados	N	79	9	Suma do campo Importe dos Billetes non Financeiros eliminados.
Importe Billetes Financeiros eliminados	N	88	9	Suma do campo Importe dos Billetes Financeiros ou tarxeta metropolitana eliminados
Importe subvencionado eliminado	N	97	9	Suma do campo <i>subvención prevista</i> (dos Billetes Financeiros eliminados) en milésimas de euro.
Número de rexistros '04'	N	106	7	Número de rexistros de Billetes Financeiros con erro (tipo de rexistro '04')
Importe Billetes	N	113	9	Suma do campo Importe dos Billetes
Financeiros con erro				Financeiros con erro
Número de rexistros de QR XENTENOVA ('05')	N	122	9	Número de rexistros de Billetes QR
Número de rexistros QR XENTENOVA ('05') con erro	N	131	9	Número de rexistros de Billetes QR -erroneos

