QONTINUUM

BOLETÍN TÉCNICO DE PRODUCTO

Código: BTP044

Título: CONACC : Acreditaciones 'DESFire' y/o 'MIFARE' en un Smartphone

Afecta a: App "Qtag_C"

Revisión: G1

Fecha: 25-9-2024

Indice:

Observaciones:

Como norma general de interpretación de este documento, toda palabra, acrónimo o frase realzada en **negrilla** que no esté subrayada tiene su explicación en el capítulo GLOSARIO DE TÉRMINOS de este documento y/o de otro cuando así se indique, mientras que las palabras, acrónimos o frases que se inicien o se escriban totalmente con mayúsculas o entre apóstrofes hacen referencia a cosas o conceptos que se presume que son del conocimiento de los lectores a los que se dirige este documento (tanto por ser de uso común como por estar explicadas en el propio documento), quedando los entrecomillados como indicación de sentido virtual o de sentido circunstancial.

QONTINUUM PLUS, s.l. se reserva el derecho de modificar todas o cualquiera de las especificaciones que se indican en este documento sin previo aviso.

R	FECHA	PÁGINA/S	OBSERVACIONES
	7-12-2015	(total)	- 1ª edición - publicación actualizable en www.qontinuum-plus.es
A	4-1-2016	(total)	- 2ª edición - ampliación del capítulo 3
B	28-1-2016	(total)	- 3ª edición - remodelado el capítulo 4
C	23-8-2016	(total)	- 4ª edición - cambio del título del documento - introducción de las Acreditaciones emuladas (App “Qtag_C”)
D	5-4-2020	(total)	- 5ª edición - nuevas restricciones (a partir de Android 10) - eliminación del subsistema SmaCPort - se corresponde con : -– Versión 1.7 (y posteriores) de la App “Qtag_C”
E	6-2-2022	(total)	- 6ª edición - remodelado el capítulo 3 - correcciones y aclaraciones
F	9-9-2022	(total)	- 7ª edición - renumeración de capítulos (el 4 y el 5 pasan a ser, respectivamente, el 6 y el 7) - nuevo capítulo 4 - nuevo capítulo 5 - correcciones y aclaraciones
F1	6-5-2024	(total)	- correcciones y aclaraciones
G	18-6-2024	(total)	- 8ª edición - correcciones y aclaraciones - se corresponde con : -– Versión 1.9 (y posteriores) de la App “Qtag_C” - utiliza el valor 9 en ‘RevPro’ (el componente “QOTF.DLL” debe ser de la Versión 2.17 o superior)
G1	25-9-2024	(total)	- correcciones y aclaraciones

1 INTRODUCCIÓN

Toda palabra, acrónimo o frase realzada en negrilla (que no esté subrayada) tiene su explicación en el capítulo 7 GLOSARIO DE TÉRMINOS de este documento.

Debido a la creciente popularización de los **Smartphone** como instrumentos de uso universal y cotidiano se está produciendo una muy rápida expansión del concepto BYOD ("Bring Your Own Device" o, en su traducción más aceptada, 'lleva-tu-propio-dispositivo'), de manera que el mundo de la seguridad se acerca a los personas al facilitar que un elemento tan socializado como lo son actualmente los **Smartphone**s pueda ser usado como **Acreditación** identificadora de todos y cada una de las personas, sin menoscabo de que otras personas puedan utilizar **Acreditaciones** basadas en soportes materiales tipo tarjeta o similar (los llamamos **Acreditaciones** de naturaleza estática nativas).

Se trata, en fín, de aceptar que hemos entrado de lleno en lo que se podría llamar la "desmaterialización" de las tarjetas tal y como las hemos conocido hasta el momento, de manera que a las muchas aplicaciones que hoy se le están dando a los **Smartphone** se une la de servir como **Acreditación** personal en el entorno del *Control de Accesos*, lo cual ha motivado que Qontinuum haya definido el **ecosistema Q-OnTheFly** para dar cabida a una serie de App que, entre otras características específicas, tienen en común que disponen de capacidad de comunicación inalámbrica con programas de aplicación desarrollados y comercializados exclusivamente por Qontinuum.

Actualmente, el **ecosistema Q-OntheFly** incluye, entre otras App, a la "Qtag_C", la cual es compatible con el **sistema CONACC**.

La App "Qtag_C" (Versión 01.nn) ha sido diseñada de manera específica para emular **Acreditaciones** 'MIFARE' tratadas en formato **fS=3** o 'DESFire' tratadas en formato **fS=3** o **fS=5** desde un **Terminal *Portátil***, de manera que los **Sujetos** puedan utilizar, en los Cabezales de lectura-escritura de la Serie 3000 y en los Terminales *Compactos* de la Serie 4000, **Acreditaciones** de naturaleza estática tanto nativas (normalmente en forma de tarjetas) como emuladas (la App "Qtag_C"), y hacerlo de manera indistinta, por lo que el uso de las **Acreditaciones** NFC (Smartphone) emuladas (soportadas por las App "Qtag_C") resulta transparente tanto para los Terminales como para los programas **OEM**, actuales y futuros.

La App "Qtag_C" (Versión 02.nn) también ha sido diseñada de manera específica para emular **Acreditaciones** 'DESFire' tratadas en formato **fS=4** desde un **Terminal *Portátil***, de manera que los **Sujetos** puedan utilizar, en los Cabezales de lectura-escritura de la Serie 3000 y en los Terminales *Compactos* de la Serie 4000, tal tipo de **Acreditaciones** (tanto de naturaleza estática como dinámica) y hacerlo de manera indistinta con otras **Acreditaciones** nativas y/o emuladas, por lo que el uso de las **Acreditaciones** 'NFC (Smartphone)' de tratamiento dinámico emuladas resulta transparente tanto para los Terminales como para el programa de aplicación.
Sin embargo, la generación y la telecarga de las **Acreditaciones** de naturaleza dinámica emuladas sólo pueden ser realizada por el programa de aplicación "QVigila" si éste tiene activados los **Módulos funcionales** modelo **Mf_4** y **Mf_EAD**, y no pueden ser realizadas por los programas **OEM**.

Los únicos requerimientos que debe satisfacer cada **Terminal *Portátil*** a ser usado por la App "QTag_C" son el estar basado en S.O. Android de la Versión 4.4.2 (o posterior) y el disponer de capacidad de comunicación vía NFC, siendo necesario que tanto los Cabezales lectores-grabadores como los Terminales utilizados en la **Instalación** sean de los modelos compatibles (fabricados por Qontinuum)[(1)] indicados en la lista www.qontinuum-plus.es/esp/soptec/infotec/_info-1.php#A9, donde también se indica la Versión de Firmware a partir de la cual resultan compatibles con las App "Qtag_C".

NOTAS:
(1) Aunque en el mercado existen muchos Cabezales lectores de otros fabricantes que permiten la lectura de elementos NFC (tipo tarjeta, 'tag', etc.), el problema que se plantea al querer utilizar **Smartphone** es el de que éstos (en su gran mayoría) no se identifican sistemáticamente con un **UID** único sino que lo hacen de manera aleatoria cada vez, por lo que no es posible establecer una relación unívoca entre cada **Smartphone** (y por tanto, el **Sujeto** que sea su **Usuario**) y, por ejemplo, el **NIS** contenido en la **Lista_Blanca** cargada en la memoria de tales Terminales o Cabezales. Por tales razones, la existencia de las estructuras **fS=4** nació, entre otras razones, para garantizar la no duplicidad.

2 LAS ACREDITACIONES

La definición de la estructura lógica que hace el **sistema CONACC** para las **Acreditaciones** 'NFC (Smartphone)' emuladas cumple con el estándar correspondiente a las **Acreditaciones** ('MIFARE' o 'DESFire') nativas, siendo éstas emuladas por la App "Qtag_C" cargada en el **Terminal *Portátil***, mientras que la arquitectura física de las **Acreditaciones** 'NFC (Smartphone)' queda establecida por la propia App y no afecta para nada a los programas **OEM** ni a los **Sujetos**.

Las **Acreditaciones** 'DESFire' de naturaleza estática nativas son entregadas inicializadas por su fabricante NXP (contienen sólo el correspondiente **UID**), de manera que ya resultan directamente operativas si no se pretende otra cosa que leer tal identificador unívoco (sería al operar en el formato **fS=3** o en el **fS=5**), mientras que si hay que grabar información en su memoria (como sería el caso de querer utilizar estructuras del tipo formato **fS=4**) se hace necesario seguir un procedimiento de emisión establecido por nuestros SDK para los programas **OEM** (la casuística para las **Acreditaciones** 'MIFARE'(1) nativas es la misma, sólo que estas contienen un **NUID**).

Las **Acreditaciones** 'DESFire' de naturaleza estática emuladas son soportadas por las App "Qtag_C", y no quedan inicializadas hasta que no se ejecuta el oportuno proceso en el cual se le asigna un **UID** que queda diferenciado de aquellos otros existentes en la **Acreditaciones** nativas, de manera que en ningún caso puede producirse una duplicidad de identificación en las **Instalaciones** que utilicen **Acreditaciones** 'DESFire' tanto nativas como emuladas. Sin embargo, si que resulta posible que se produzcan duplicados del **NUID** en aquellas **Instalaciones** que utilicen **Acreditaciones** 'MIFARE' tanto nativas como emuladas(1), por lo que los responsables de las **Instalaciones** que las estén usando deberían considerar un plan de migración para abandonar el uso de las **Acreditaciones** 'MIFARE'.

Las **Acreditaciones** 'DESFire' de naturaleza dinámica emuladas son soportadas sólo por las App "Qtag_C" sin que deban ser ni **Prepersonalizadas** ni **Personalizadas** dado que las correspondientes estructuras del tipo formato **fS=4** son generadas por el programa de aplicación "QVigila" y telecargadas directamente en las oportunas App "Qtag_C" mediante comunicaciones encriptadas.

NOTAS:
(1) La problemática existente con las **Acreditaciones** 'MIFARE' queda expuesta en un archivo PDF que se encuentra en www.qontinuum-plus.es/esp/soptec/infotec/_info-3.php#A9, pero, a diferencia de lo que ocurre con las **Acreditaciones** 'MIFARE' nativas, las emuladas por medio de la App "Qtag_C" no son clonables dado que en la comunicación entre nuestros Cabezales y las **Acreditaciones** 'NFC (Smartphone)' dotadas con la App "Qtag_C" no usamos el algoritmo de encriptación 'CRYPTO1' sino el algoritmo AES-128.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

3 LA EMISIÓN ...

Por obvias razones de seguridad, las App "Qtag_C" cargadas en los **Smartphone** no pueden ser usadas directamente como **Acreditaciones** emuladas sino que antes deben ser inicializadas, validadas y preparadas de manera conveniente para que puedan ser utilizadas con total seguridad, para lo cual se utiliza tanto el **IMEI** como el **ICCID**.

Una vez cargada la App "Qtag_C" en el **Smartphone**, y para inicializar el tipo de **Acreditación** deseada, existen dos escenarios posibles en razón del origen del programa de aplicación usado en la **Instalación**, siendo en modo local (subcapítulo 3.1) la realizada desde el programa de utilidad "Q2_UTIL" y siendo el modo remoto (subcapítulo 3.2) la realizada desde el programa de aplicación "QVigila".

3.1 ... en modo local

Este modo de emisión resulta aplicable en aquellas **Instalaciones** donde el esquema de uso sea de tipo cerrado (por ejemplo, su propio edificio o centro de trabajo) para lo cual hay que utilizar la opción {SAT : NFC (Smartphone)} del programa de utilidad "Q2_UTIL" de la Versión 8.1 o posterior (ver la correspondiente Ayuda en tal programa) así como un Terminal *de Sobremesa* modelo DEF-3311 conectado al mismo PC en el que se ejecute el programa de utilidad "Q2_UTIL".

Por medio de tal opción es posible inicializar cada **Acreditación** 'NFC (Smatphone)' de manera que pueda emular tanto **Acreditaciones** 'MIFARE' (en formato **fS=3** o en formato **fS=4**) como **Acreditaciones** 'DESFire' (en formato **fS=3** o en formato **fS=4** o en formato **fS=5**), así como también permite visualizar información básica de todas las instancias de emulación que consten archivadas en la App (pertenecientes a la misma **Instalación**).

Al ser inicializada, la **Acreditación** emulada quedará en la misma situación en la que se encuentran las **Acreditaciones** nativas cuando son recibidas del proveedor, por lo que a partir de ese momento hay que actuar en función del formato **fS=n** que se utilice en la **Instalación**.

3.1.1 emulación de los formatos fS=3, fS=4 y fS=5

Dado que se trata de los formatos naturales de las **Acreditaciones** emuladas, y una vez finalizado el proceso de inicialización, no es necesario realizar nada más puesto que la propia App "Qtag_C" ha asignado a la **Acreditación** emulada un **NUFAB** específico (generado de manera aleatoria)(1).

3.1.2 emisión en formato fS=4

Los procedimientos lógicos necesarios para la emisión en formato **fS=4** de las **Acreditaciones** emuladas por la App "Qtag_C" son exactamente los mismos que los necesarios para las correspondientes **Acreditaciones** nativas, siendo la metodología que hay que seguir la explicada en el capítulo 3 de la Revisión L (y posteriores) del documento BTP031. De esta manera, y desde el punto de vista del operador del programa **OEM**, no hay diferencia alguna en la manera en la que debe proceder para la **Prepersonalización** y para la **Personalización** de las **Acreditaciones** dado que es exactamente la misma tanto si son nativas como si son emuladas.

NOTAS:

(1) Dado que el proceso de inicialización de las App "Qtag_C" se realiza por medio del programa de utilidad "Q2_UTIL" y no por medio de un programa de aplicación, no hay manera de conocer durante tal proceso si el **NUFAB** asignado estará o no estará repetido en la **Instalación**, lo cual resulta en ser la misma casuística que se puede producir cuando se utilizan **Acreditaciones** 'MIFARE' *Classic* nativas dado que actualmente existen varios fabricantes que no siguen un criterio común para la asignación de los **NUFAB**, por lo que tal código debe ser considerado como un **NUID**.

3.2 ... en modo remoto

Este modo de emisión resulta aplicable en aquellas **Instalaciones** donde el esquema de uso sea de tipo abierto (por ejemplo, múltiples edificios y/o recintos repartidos geográficamente), para lo cual hay que utilizar la pestaña {Gestión : Usuarios / Edición [App "Qtag_C"]} del programa de aplicación "QVigila" de la Versión 1.1 o posterior (ver la correspondiente Ayuda en tal programa).

Por medio de tal opción es posible inicializar cada **Acreditación** 'NFC (Smatphone)' de manera que pueda emular tanto **Acreditaciones** 'DESFire' (en formato **fS=3** o en formato **fS=4** o en formato **fS=5**) como **Acreditaciones** 'MIFARE' (en formato **fS=3** o en formato **fS=4**).

Al ser inicializada, la **Acreditación** emulada quedará en la misma situación en la que se encuentran las **Acreditaciones** nativas cuando son recibidas del proveedor, por lo que a partir de ese momento hay que actuar en función del formato **fS=n** que se utilice en la **Instalación** (los pasos necesarios para la inicialización remota se exponen en el capítulo 4).

3.2.1 emulación estática de los formatos fS=3, fS=4 y fS=5

Se trata de los formatos naturales de las **Acreditaciones** emuladas, y una vez finalizado el proceso de inicialización, no es necesario realizar nada más puesto que la propia App "Qtag_C" ha asignado a la **Acreditación** de naturaleza estática emulada un **NUFAB** específico (generado de manera aleatoria) pero autorizado(1) en tiempo real por el **Servidor QOTF**.

3.2.2 emulación dinámica del formato fS=4

Una vez cargada la App "Qtag_C" en el **Terminal *Portátil*** resulta posible generar una **Acreditación** 'DESFire'de naturaleza dinámica emulada (en formato **fS=4**)(2) por parte del programa de aplicación "QVigila", de manera que éste provoca el establecimiento de **sesión segura** de comunicaciones con la App "Qtag_C" para telecargar, con la máxima seguridad posible, una **Acreditación** emulada de naturaleza dinámica en el **Terminal *Portátil*** del **Sujeto** (tal **Acreditación** se carga completa, esto es con la correspondiente **Prepersonalización** y **Personalización** efectuadas).

NOTAS:
(1) Es en el proceso de inicialización cuando las App "Qtag_C" negocian con el **Servidor QOTF** el valor que finalmente quedará asignado como **NUFAB**, de manera que el **Servidor QOTF** rechaza todos aquellos valores que le sean propuestos pero que ya existan en la Base de Datos "Fenix" asignados a cualquier otra **Acreditación** que ya estuviera registrada, tanto las de naturaleza estática (nativas o emuladas) como las de naturaleza dinámica.

(2) El uso de **Acreditaciones** de naturaleza dinámica emuladas en formato **fS=4** sólo se contempla para **Instalaciones** que utilicen **Acreditaciones** 'DESFire', de manera que no es posible para **Instalaciones** que utilicen **Acreditaciones** 'MIFARE' dado que, de manera genérica, no se pueden considerar seguras, por cuya razón desaconsejamos su uso.

4 LA INICIALIZACIÓN REMOTA

El proceso de inicialización remota de la App “Qtag_C” es genérico para cualquier tipo de **Smartphone**, pero en aquellos equipos en los que la Versión de Android sea la 6 (y posterior pero anterior a la Versión 10) hay que tener en cuenta las estrictas restricciones implementadas(1), mientras que en aquellos equipos en los que la Versión de Android sea la 10 (y posterior) hay que tener en cuenta las más estrictas restricciones implementadas(2).

El programa de aplicación “QVigila” dispone de la pestaña {Gestión : Usuarios / Edición [App “Qtag_C”]}, la cual permite registrar los datos básicos del **Smartphone** que el potencial **Usuario** pretenda utilizar como **Acreditación**, así como preparar la información necesaria para que cada App “Qtag_C” resulte inicializada y acabe siendo operativa como **Acreditación** de naturaleza estática y siendo reconocida como tal por los Terminales del **sistema CONACC**.

Los pasos necesarios para lograr tal pretensión son los siguientes:

P1) El demandante que pretenda disponer de un **Smartphone** como medio físico de identificación (para ser considerado como **Usuario** por el programa de aplicación “QVigila”) debe cargar primero la App “Qtag_C” en su **Smartphone** desde “Google Play Store”.

P2) El demandante debe comunicar, a quién corresponda en la **Instalación** y por el medio que se haya establecido, los datos identificativos básicos del **Usuario**, así como la CLAVE1 y la CLAVE2 de su **Smartphone** (ambos los facilita la propia App “Qtag_C”(3)).

P3) Los datos del **Usuario** deben ser dados de alta en la subopción {Gestión : Usuarios / Edición [General]} del programa de aplicación “QVigila”, mientras que la CLAVE 1 y la CLAVE 2 deben ser anotadas en la pestaña {Gestión : Usuarios / Edición [App “Qtag_C”]}, generándose en consecuencia una ‘Clave de Autorización’ de cuatro Bytes en hexadecimal.

P4) Alguien en la **Instalación** deberá enviar tal ‘Clave de Autorización’ al potencial **Usuario** además de indicarle cuál es la información que debe usar para conectarse con el **Servidor QOTF** (Dirección IP, Puerto TCP, etc.).

P5) Cuando el potencial **Usuario** establezca conexión deberá anotar en la App “Qtag_C” la ‘Clave de Autorización’ que se le haya indicado.

P6) Si la ‘Clave de Autorización’ es aceptada, el **Servidor QOTF** establece con la App “Qtag_C” una sesión de intercambio de tramas encriptadas, pudiendo darse, en el transcurso de tal sesión, alguna de las situaciones cuyas causas aparecen en el siguiente cuadro (también aparecen los CE de los marcajes generados, los cuales quedan archivados en la Base de Datos ‘Fenix’) así como los **mensajes de tipo 1** que aparecen en la App “Qtag_C”:

CE=	mensaje :	causa :
223000024	< “Qtag_C” : rechazada >	Debido a que no se considera válida la petición o a que en la Base de Datos ‘Fenix’ no existe información vinculante o es insuficiente, el **Servidor QOTF** no ha reconocido a la App “Qtag_C” cuando esta pretende ser activada para poder operar como **Acreditación** 'NFC (Smartphone)'.
223000025	< Error de activación en la App >	- El **Servidor QOTF** ha sido informado por la App “Qtag_C” de que esta no ha quedado activada por problemas internos (por ejemplo, falta de memoria disponible en el **Smartphone**).

CE=	mensaje :	causa :
223000026	< Existe activación previa de la Acreditación >	- El **Servidor QOTF** ha sido informado por la App “Qtag_C” de que la inicialización que se pretende no es posible dado que ya existe otra de iguales características.
223000061	< "Qtag_C" : puede ser usada >	La App “Qtag_C” ha informado al **Servidor QOTF** que la **Acreditación** 'NFC (Smartphone)' del **Usuario** ya puede ser usada dado que ha completado la inicialización (en el formato **fS=3** o en el formato **fS=5**) o ha completado la **Personalización** (en el formato **fS=4**).
223000062	< "Qtag_C" : NUFAB existente >	El **Servidor QOTF** ha recibido de la App “Qtag_C” el **NUFAB** generado por esta en el proceso de inicialización (para el formato **fS=3** o el formato **fS=5**) o en el proceso de **Personalización** (para el formato **fS=4**), pero tal **NUFAB** ya existe en la Base de Datos ‘Fenix’ (asignado al mismo **Usuario**, asignado a otro **Usuario** o como **Acreditación** anulada), por lo que, en cualquier caso, es necesario que alguien responsable del **subsistema IRPA** investigue el problema y aplique la mejor solución correctiva.

P7) Si el proceso de inicialización ha podido ser llevado a cabo, el resultado final será distinto dependiendo de si se ha realizado la inicialización de la App “Qtag_C” para emular una **Acreditación** en formato **fS=3** o en formato **fS=5** (sigue en p7.1) o de si se ha realizado la **Personalización** de una **Acreditación** en formato **fS=4** (sigue en p7.2):

P7.1) Al terminar correctamente el proceso de inicialización, el **Servidor QOTF** habrá registrado el **NUFAB** enviado (de manera encriptada) por la App “Qtag_C” y habrá generado un **marcaje normal** con CE=223000061, de manera que, a partir de tal momento, la App “Qtag_C” será por completo operativa como **Acreditación** emulada en formato **fS=3** (si se trata de una **Instalación** basada en **Acreditaciones** que usen **NUID**) o en formato **fS=5** (si se trata de una **Instalación** basada en **Acreditaciones** que usen **UID**).

P7.2) Al terminar correctamente el proceso de **Personalización**, el **Servidor QOTF** habrá generado una estructura **fS=4** (conteniendo el correspondiente **INST1**, **NIS** y demás información) y la habrá enviado, de manera encriptada, a la App “Qtag_C” y habrá generado un **marcaje normal** con CE=223000061, de manera que la App “Qtag_C” será por completo operativa como **Acreditación** emulada de naturaleza estática o como **Acreditación** de naturaleza dinámica emulada .

P8) A partir de este momento, el **Smartphone** adquiere la categoría de **Acreditación** dentro del **ecosistema Q-OnTheFly** y dentro del **sistema CONACC**, por lo que, a todos los efectos, se comportará de manera estándar.

NOTAS:
(1) En las diversas implementaciones del S.O. Android (anteriores a la Versión 6) a las que hemos tenido acceso, nuestras App (y cualquier otra del mercado) disponen de permisos explícitos (solicitados al ejecutar por primera vez la App) para acceder líbremente a ciertos recursos. Sin embargo, a partir de la aparición de la Versión 6 de Android, se han aplicado más restricciones de uso a ciertos recursos (como son la lectura del **IMEI** y del **ICCID**), de manera que ahora, al arrancar por primera vez y sólo si la Versión del S.O. es 6 o posterior (pero anterior a la Versión 10), nuestras App muestran el siguiente **mensaje de tipo 1**, el cual debe ser aceptado:

> Solicitud de permisos.
> Por favor, acepte el permiso que se le solicitará a continuación.
> Tal permiso es necesario para que la App pueda leer el IMEI del Smartphone (CLAVE 1) y el ICCID de la tarjeta SIM (CLAVE 2).

Hay que tener muy en cuenta que el **mensaje de tipo 0** que aparecerá a continuación de tocar en el botón [Continuar] es el que cada fabricante ha introducido en su implementación de Android, de manera que en algunos **Smartphone** puede resultar razonablemente esclarecedor mientras que en otros (como en el caso de la marca Samsung) puede inducir a confusión dado que indica que la App puede realizar llamadas telefónicas, lo cual, aun siendo cierta la posibilidad, no es aplicable a las App “Qtag_C”.

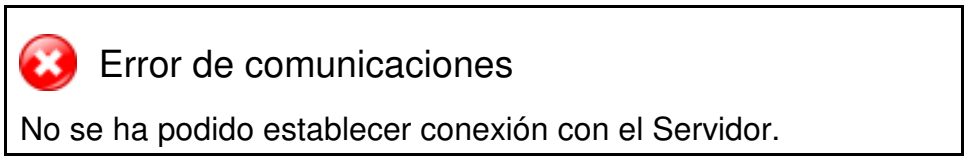
(2) Debido a nuevas restricciones implantadas por el S.O. Android 10 (y posteriores), no resulta posible acceder ni al **IMEI** ni al **ICCID**, por lo que tales valores pasan a ser virtuales al ser fruto de una generación aleatoria ejecutada por la App “Qtag_C”.
Si fuera el caso de que cuando el **Smartphone** hubiera sido dado de alta en el programa de aplicación aquel tuviera una Versión del S.O. Android anterior a la 10, tal **Smartphone** deberá ser dado de alta de nuevo dado que el IMEI y el ICCID originales son ahora, y por razones de seguridad, inaccesibles, de manera que han sido substituidos por las llamadas CLAVE1 y CLAVE2 (códigos generados de manera aleatoria por la propia App).

(3) La introducción de la CLAVE1 y de la CLAVE2 en el programa de aplicación permitirá, posteriormente, la identificación de cada App que se conecte y permitirá facilitar a tal App la autorización necesaria para operar con los Terminales del **sistema CONACC** como **Acreditación** emulada de naturaleza estática o como **Acreditación** de naturaleza dinámica emulada.

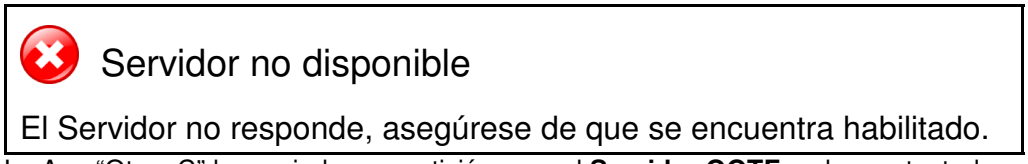
ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

5 SITUACIONES DE ERROR

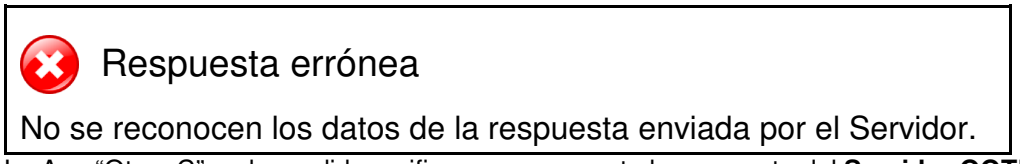
Dado que las comunicaciones inalámbricas están en la base del **Servidor QOTF**, y aunque el protocolo implementado es muy robusto, hay que asumir que en ocasiones (y de manera inevitable como cuando exista mala cobertura), se producirán errores, los cuales son informados por las App "Qtag_C" a los **Sujetos** mediante **mensajes de tipo 1** y de la manera expuesta a continuación:



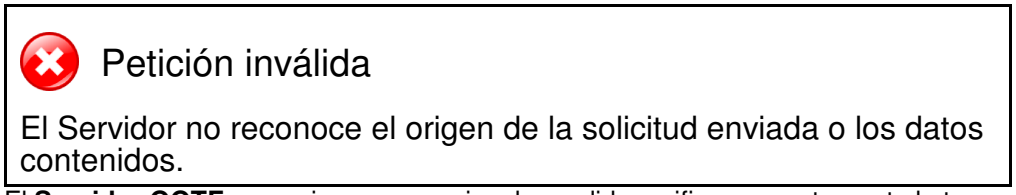
Se ha producido una excepción en la App "Qtag_C" al intentar abrir el 'socket' para comunicar con el **Servidor QOTF** (la dirección IP o el Puerto indicados no están disponibles). También aparece si el **Smartphone** no dispone de conexión a una red.



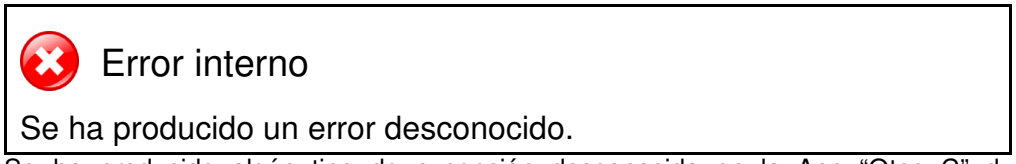
La App "Qtag_C" ha enviado una petición pero el **Servidor QOTF** no ha contestado antes del tiempo indicado en el campo Espera conexiones (en segundos), por lo que la App "Qtag_C" ha cerrado la comunicación. Esto puede deberse a que se ha producido algún tipo de excepción en el **Servidor QOTF** al recibir y verificar la trama o al intentar generar la respuesta o a que no esté operativo o a que hay que esperar más tiempo del indicado.



La App "Qtag_C" no ha podido verificar como correcta la respuesta del **Servidor QOTF**.



El **Servidor QOTF** comunica un error si no ha podido verificar correctamente la trama recibida de la App "Qtag_C" (este error debe ser comunicado a Qontinuum) .



Se ha producido algún tipo de excepción desconocida en la App "Qtag_C" durante la comunicación como *Cliente* (este error debe ser comunicado a Qontinuum).

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

6 LA SEGURIDAD

Las aplicaciones cargadas en un **Smartphone** gozan de la seguridad intrínseca que les aporta el S.O. sobre el que operan (en este caso de trata de Android de la Versión 4.4.2 o posterior), además de utilizar sólo comunicaciones seguras en base a encriptación mediante AES-128.

Dado que para los Terminales de Qontinuum no existe diferencia funcional tanto si las **Acreditaciones** son de naturaleza estática (nativas o emuladas) como si son de naturaleza dinámica, los Terminales (tanto *Modulares* como *Compactos*) de la Familia DEF tratan a todas las **Acreditaciones** de la misma manera, incluso si se trata de **Acreditaciones** 'MIFARE'(1)

En toda **Instalación**, y bajo el punto de vista de la seguridad, hay que analizar con detenimiento la vulnerabilidad de todos y cada uno de los puntos de acceso, de manera que en aquellos en los que se considere la necesidad de disponer de alta seguridad sólo deberían ser aceptadas **Acreditaciones** 'DESFire EVn' de naturaleza estática (nativas o emuladas) así como **Acreditaciones** de naturaleza dinámica, cuya arquitectura es 'DESFire' tratadas en formato **fS=4**, exclusivamente.

Además, y si el punto de acceso debe ofrecer una muy alta seguridad, se hace necesario forzar algún tipo de autenticación mediante **IDEP** (especialmente por biometría), siendo en tal caso por completo factible la utilización también de **Acreditaciones** de naturaleza estática (nativas o emuladas) y/o de **Acreditaciones** de naturaleza dinámica emuladas (vía App "Qtag_C").

NOTAS:
(1) La emulación de **Acreditaciones** 'MIFARE' (de naturaleza estática) por medio de la "App Qtag_C" goza de la misma seguridad que la emulación de las **Acreditaciones** 'DESFire' dado que en las comunicaciones con los Cabezales no se utiliza la encriptación CRYPTO1 sino AES-128.

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE

7 GLOSARIO DE TÉRMINOS

Todos los términos que se explican a continuación lo son de una manera no exhaustiva, por lo cual es posible que para entender totalmente a alguno de ellos deba acudirse a aquellas partes de texto en las que resulten referidos.

Algunos de los términos pueden encontrarse en el texto anterior (y en el propio GLOSARIO) tanto en singular como en plural, siendo su explicación la misma para ambos casos.

El significado que se asigna a alguno de los siguientes términos hay que entenderlo como exclusivamente referido al texto global, de manera que en otro contexto pueden significar otras cosas (incluso totalmente contradictorias) a las aquí explicadas.

La siguiente lista está clasificada en base al código IA5 del CCITT/ISO.

Acreditación

De manera genérica, reciben este nombre cualesquiera de los elementos cuya funcionalidad original es la de servir como soporte de información para la simple identificación visual (mediante nombre, foto, etc.) de los **Sujetos**, siendo sin embargo la funcionalidad más deseada la de facilitar la identificación automática por parte de sistemas electrónicos que son capaces de leer la información contenida en tales elementos, los cuales actualmente (y casi exclusivamente) comunican tal información vía radio (RFID) en transmisiones de muy corto alcance.
Las *Acreditaciones* pueden ser de naturaleza estática nativa (fabricados por terceros), en las cuales tanto el Circuito Integrado (CI) como la correspondiente antena están contenidos en una pieza de plástico del tamaño y grosor de una tarjeta de crédito o débito convencional (y por tanto cumpliendo con la norma ISO 7810) o contenidos en un elemento plástico como un colgante o llavero, pero las *Acreditaciones* de naturaleza estática también pueden ser emuladas por una App “Qtag_C” (cargada en un **Smartphone**).
Además, también pueden ser utilizadas *Acreditaciones* de naturaleza dinámica, las cuales son cargadas telemáticamente en un **Smartphone** y gestionadas por los **Sujetos** directamente en un menú de la App “Qtag_C”, siendo condición necesaria que tales **Smartphone** dispongan de comunicaciones 3G/4G y NFC.
A efectos tanto de los **Sujetos** como de los sistemas, tanto las *Acreditaciones* emuladas como las *Acreditaciones* de naturaleza estática se comportan igual, siendo posible la convivencia y el uso indiscriminado de los tres tipos de *Acreditaciones* (estáticas nativas, estáticas emuladas y dinámicas emuladas) en cualquiera lugar en el que el correspondiente Cabezal lector-grabador resulte compatible según lo indicado en el capítulo 1.

Clave de sesión

El valor que establecen entre ellos el programa “QVigila” y cada App “Qtag_C” para garantizar el posterior reconocimiento mutuo en las sesiones de comunicación, de manera que cada vez se establezca una **sesión segura** de comunicaciones.

ICCID

Acrónimo en inglés de Integrated Circuit Card IDentifier.
Es un número grabado en la SIM de todo **Smartphone**, y si estableciéramos un símil con las redes, el ICCID sería equivalente a la MAC de un dispositivo (al identificar la interfaz física).
Este número es el que se utiliza, entre cosas, para identificar al país, a la red y a la propia tarjeta, y es único.
Todos los números del ICCID empiezan por 89 y van seguidos por el identificador del país de emisión, Una característica (anti clonación) de este número es que va ligado a la SIM; si se estropea o se pierde la tarjeta hay que generar otra SIM que, por lo antedicho, presentará un ICCID distinto.

IDEP

Acrónimo de Interacción De las Personas.
La indicación a cada Terminal de cómo debe ser (si debe haberla) la manera en la que los **Usuarios** se autentiquen una vez acabada la fase de validación de la **Acreditación**, siendo las principales por anotación de un **PIN** o por presentación biométrica.

IMEI

Acrónimo en inglés de International Mobile Equipment Identity.
Se trata de un identificador único para los **Smartphone**s, entre otros equipos de comunicaciones.

INST1

El código que identifica y diferencia a las **Instalaciones**, por lo cual es irrepetible excepto para una misma **Instalación**.
Este código lo asigna Qontinuum y es público.

Instalación

Asignamos este nombre a toda Organización que utiliza alguno de nuestros productos.
Cada *Instalación* es única para los sistemas de Qontinuum, y está identificada y diferenciada de otras por el valor del **INST1**.

Lista_Blanca

La relación de **Acreditaciones** (tanto nativas como emuladas) identificadas por su **NIS** que deben ser consideradas por el Firmware del Terminal de tipo fijo como susceptibles de tener acceso siempre y cuando cumplan con una serie de condiciones de validación cuya base de partida está indicada en la propia Lista.

Módulo funcional

En algunos de los programas de aplicación de qontinuum puede ser que ciertas prestaciones no se encuentren disponibles de manera básica sino como funcionalidad activable, por lo que (en razón de la conveniencia de su uso) pueden ser adquiridos posteriormente y quedar vinculados al programa de aplicación mediante un mecanismo de actualización por clave, pudiendo tal adquisición suponer contraprestación económica.

Mf_4

Asignamos tal nombre al **Módulo funcional** que permite que el programa de aplicación “Qvigila” trate **Acreditaciones** dotadas con estructuras **fS=4**, por lo que, una vez activado este recurso, pasan a ser operativas varias opciones especializadas del programa de aplicación.
Para usar este recurso es necesario disponer de autorización expresa en el elemento “G-SECUR” así como también disponer del **Módulo funcional** modelo **Mf_CTF**.

Mf_CAV

Asignamos tal nombre (**C**ontrol de **A**ccesos **V**ísitantes) al **Módulo funcional** que puede formar parte del programa de aplicación “QVigila”, siendo su misión la de gestionar todos los recursos implementados para la gestión y el control de los **Visitantes**.

Mf_CTF

Asignamos tal nombre (**C**omunicador para **T**erminales de tipo **F**ijo) al **Módulo funcional** que puede formar parte del programa de aplicación “QVigila”, siendo su misión la de comunicar con los Terminales (de tipo fijo) para el *Control de Accesos* (y también para el *Control de Presencia*) así como la de gestionar todos los recursos que les afecten.

Mf_EAD

Asignamos tal nombre (**E**misión de **A**creditaciones **D**inámicas) al **Módulo funcional** que puede formar parte del programa de aplicación “QVigila” y dotarlo así del potencial de generación de **Acreditaciones** de naturaleza dinámica emuladas.

NIS

Acrónimo de Número Identificativo Serializado.
El identificador imprescindible que singulariza a todas las **Acreditaciones** en una misma **Instalación**.
En la estructura **fS=4** ocupa 4 Bytes.

NUFAB

Acrónimo de NÚmero de FABrica.
Se refiere al dato obtenido tanto de las **Acreditaciones** 'MIFARE' como de las 'DESFIre' y que se utiliza para procesos internos relacionados con la seguridad. Para 'MIFARE' corresponde a los cuatro Bytes del **NUID**, mientras que para 'DESFire' se compone del Byte CT (Cascade Tag) seguido de los siete Bytes del **UID**.
También es conocido como 'Número de Serie' o CSN (Chip Serial Number).

NUID

Acrónimo en inglés de Non-Unique IDentifier.
La numeración interna de las **Acreditaciones** 'MIFARE' *Classic*, siendo de 4 Bytes y con posibilidad de que existan duplicados al ser diversos los fabricantes que las producen actualmente; opcionalmente también lo utilizan las **Acreditaciones** 'MIFARE' *Plus nivel 1* y 'MIFARE' *Classic EV1*.

OEM

Acrónimo en inglés de Original Equipment Maker.
Se usa (vulgarmente en inglés) para referirse a aquellas empresas que utilizan elementos de otras (Hardware y/o Software) para añadirles valor y ofrecerlas como equipos o sistemas originales.
Por extensión también reciben este nombre sus propios programas.

PIN

Acrónimo en inglés de Personal Identification Number.
Se usa (vulgarmente en inglés) para referirse al número de identificación personal.
Es el código numérico que sirve para que el **Usuario** de la **Acreditación** (tanto nativa como emulada) se autentique personalmente en aquellos Terminales que dispongan de teclado y cuyo Firmware lo requiera.
El número de identificación personal admite valores entre 0000 y 9999, siendo su uso opcional en función del tipo de Terminal.

Personalización

La causa y el efecto que permiten que las **Acreditaciones** (tanto nativas como emuladas) que estén **Prepersonalizadas** resulten plenamente operativas. La causa reside en la utilización de los recursos del **sistema CONACC** implementados por el programa de aplicación para realizar la carga de los datos en los archivos de la estructura **fS=4**, de manera que, como efecto, cada una de tales **Acreditaciones** pase a contener información válida que define por completo a su **Usuario** en la **Instalación**, por lo que pueden ser utilizadas en el sistema.

Prepersonalización

La causa y el efecto que permiten que las **Acreditaciones** (tanto nativas como emuladas) queden preparadas para su **Personalización**. La causa reside en la utilización de los recursos del **sistema CONACC** implementados por el programa de aplicación o por el programa de utilidad DELTA/1, siendo el efecto la formalización de la estructura **fS=4** (actualmente, el programa de utilidad DELTA/1 y el programa de utilidad DELTA/3, al igual que un Terminal *de Sobremesa*, sólo forman parte de los Kit modelo DEF-500, siendo imprescindible uno de ellos en toda **Instalación**).

Servidor QOTF

Este Servicio de Windows es el encargado de actuar como *Servidor* para algunas App del **ecosistema Q-OnTheFly** (accediendo por su cuenta a la Base de Datos 'Fenix'). El *Servidor QOTF* puede ser instalado en cualquier equipo de la **Instalación**, siendo necesario que tal equipo tenga visibilidad en la red.

Sujeto

En el entorno del **ecosistema Q-OnTheFly** se llama así a cualquier persona que deba estar bajo el control del programa de aplicación, tanto si se trata de un **Usuario** como si se trata de un **Visitante**.

Smartphone

El nombre genérico aplicado al equipo telefónico que está dotado con notables recursos tecnológicos, siendo como mínimo necesario, para el uso de la App "Qtag_C", que opere bajo S.O. Android 4.4.2 (o posterior) y que disponga de capacidad de comunicación vía NFC.

Terminal *Portátil*

En el entorno del programa de aplicación "QVigila" recibe este nombre el **Smartphone** en el que se ha cargado la App "Qtag_C".

Usuario

Reciben este calificativo todas aquellas personas que, formando parte del personal de la **Instalación** o no (por ejemplo, personal que pertenezca a empresas subcontratadas), deben ser identificadas, mediante su **Acreditación** y de manera inequívoca, por el *Control de Accesos*.

UID

Acrónimo en inglés de Unique IDentifier.
La numeración interna de las **Acreditaciones** 'DESFire EV1, 'DESFire EV2 y 'DESFire EV3, siendo de 7 Bytes y sin posibilidad de que existan duplicados al ser sólo NXP el fabricante que las produce.
También lo utilizan los **Smartphone** en el nivel básico de comunicación NFC, siendo entonces un número aleatorio mientras tal **Acreditación** emulada por medio de la App "Qtag_C" no haya sido inicializada por medio del programa de utilidad "Q2_UTIL" o por medio del programa de aplicación "QVigila", a partir de cuyo momento pasa a ser un número fijo e irrepetible.

Visitante

Reciben este calificativo todas aquellas personas que no pertenecen a la **Instalación**, las cuales no disponen de una **Acreditación** asignada de manera permanente sino de una que reciben al entrar y que deben devolver al salir.
Para su funcionamiento es necesario que el **Módulo funcional** modelo **Mf_CAV** esté activado.

ecosistema Q-OnTheFly

El nombre asignado al entorno operativo en el cual intervienen tanto algunas de nuestras App (para aquellos **Smartphone** que dispongan de capacidad NFC de lectura-grabación de **Acreditaciones** y de comunicaciones inalámbricas de datos tanto vía telefónica como vía WiFi) como intervienen algunos de nuestros programas de aplicación, basados en PC, así como el **Servidor QOTF** (el cual actúa como Servidor para tales App), todo ello utilizando recursos básico del **sistema CONACC** pero sin habilitación de uso para los **OEM**.

fS=3

El nombre propio asignado a las estructuras estándar de las **Acreditaciones** 'MIFARE', lo cual implica que las **Acreditaciones** son utilizadas tal cual han sido fabricadas (o emuladas), tomando el **NUFAB** como **NIS** de 4 Bytes.

fS=4

El nombre propio asignado a las estructuras de información y tratamiento que cumplen con la especificación de Qontinuum para las **Acreditaciones** que permiten la lectura pero también la grabación de información en "tiempo real de uso". Cuando afecta a los elementos 'DESFire' (o 'MIFARE') nativos, y dependiendo de su memoria disponible, pueden contener una o más de tales estructuras que contienen toda la información correspondiente al **Sujeto** y que resulta relevante para un eficaz *Control de Accesos* de funcionamiento desatendido (no permanentemente supervisado por el programa de aplicación).

fS=5

El nombre propio asignado a la estructura estándar de las **Acreditaciones** 'DESFire', en las cuales el **UID** ocupa 56 bits aunque se reservan 7 bits más, por lo que el **NUFAB** pasa a requerir 8 Bytes en todas las Listas y Tablas en las que esté involucrado.

fS=n

El nombre común asignado a las estructuras de información definidas por Qontinuum para ser usadas en sus equipos; en **Acreditaciones** de naturaleza estática (nativas o emuladas) sólo son posibles los formatos **fS=3**, **fS=4** y **fS=5**, mientras que en **Acreditaciones** de naturaleza dinámica emuladas sólo es posible el formato **fS=4**.

mensaje de tipo 0

Los inherentes al S.O. (aparecen en el idioma en el cual esté operando el **Terminal *Portátil***).

mensaje de tipo 1

Los mostrados por la App (en el idioma del S.O. pero sólo para Catalán, Español e Inglés, de manera que para otros idiomas se utiliza el Inglés como idioma por defecto).

sesión segura

La situación que se produce como consecuencia del reconocimiento mutuo de la **Clave de sesión** entre el programa de aplicación "QVigila" y la App "Qtag_C", siendo la situación necesaria para formalizar todas las comunicaciones encriptadas que son necesarias para la identificación de tales App.

sistema CONACC

El conjunto de especificaciones y normas definidas para ser aplicadas a un entorno de *Control de Accesos*, de *Control de Presencia* y/o de *Captura de Datos en Planta* y que han sido establecidas para otorgar las mayores facilidades de diseño y de programación tanto a Qontinuum como a los **OEM**.

El sistema implica Hardware específico y Software (programas de utilidad e instrumentos de soporte para plataformas Windows de 32/64 bits).

ESTA PÁGINA HA SIDO DEJADA EN BLANCO INTENCIONADAMENTE