

MANUAL DE USUARIO

GESTOR DE TARJETAS A.C.A.

Elaborado por: IT-CGAE

Fecha: 03/03/2006

Revisado por:

Fecha:

Aprobado por:

Fecha:

Versión: 1.2

1. HISTORICO DE VERSIONES

DESCRIPCIÓN	FECHA	VERSIÓN
Elaboración inicial del documento	04/05/2005	1.0
Revisión y actualización del documento	08/07/2005	1.1
Mejora: autoactualización on-line de la aplicación	13/09/2005	1.2

INDICE

1. HISTORICO DE VERSIONES.....	2
2. INTRODUCCIÓN	4
2.1. OBJETIVO	4
2.2. ALCANCE.....	4
2.3. DESCRIPCIÓN.....	4
2.4. ABREVIATURAS	5
3. VENTANA PRINCIPAL:	6
3.1. DESCRIPCIÓN:.....	6
3.2. OPERACIÓN:	7
4. MENÚ ID'S DIGITALES:	10
4.1. IMPORTAR CERTIFICADO	11
4.2. IMPORTAR ID DIGITAL:	12
4.3. BORRAR OBJETO:	13
4.4. mostrar ids digitales:	14
5. MENÚ TARJETA:	16
5.1. Desbloquear pin:.....	16
5.2. cambiar pin:	17
5.3. cambiar pUK:.....	18
6. MENÚ AYUDA:.....	18
6.1. información de las versiones:	18
6.2. acerca de:	19
7. DOCUMENTACIÓN DE REFERENCIA	¡Error! Marcador no definido.

2. INTRODUCCIÓN

2.1. OBJETIVO

El presente documento se elabora con el fin de describir detalladamente la utilización y las funcionalidades de la aplicación GTA (gestor de tarjetas A.C.A.).

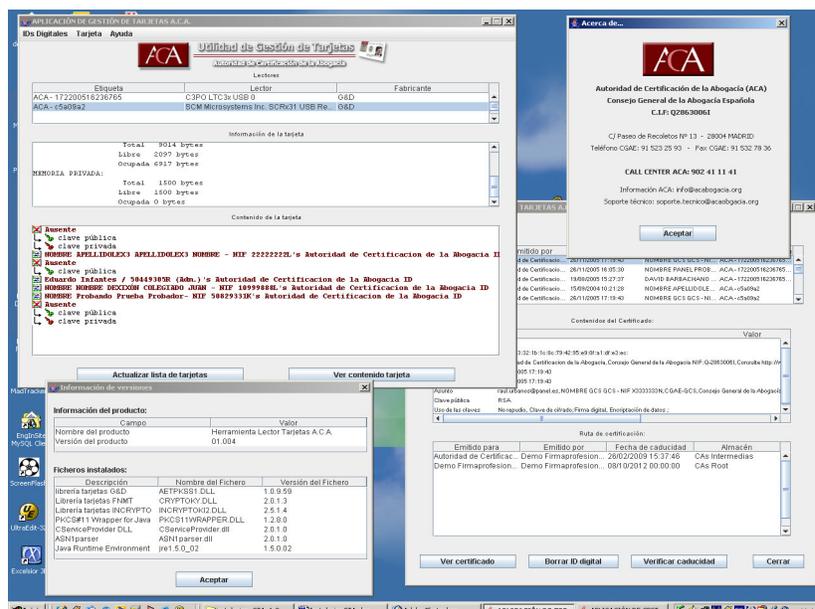
2.2. ALCANCE

Este documento va dirigido a los usuarios de la aplicación GTA, para que aprendan el manejo de la misma. Se tratarán cada una de las funcionalidades por separado, observando las diferentes posibilidades que puedan darse en ellos. Hemos estructurado este manual por el orden que en el que las opciones se distribuyen en los menús tienen la aplicación.

2.3. DESCRIPCIÓN

GTA es una aplicación dirigida a usuarios de tarjetas Smart Card contenedoras de certificados, con interfaz de acceso que sigue el estándar PKCS11, que les permitirá gestionar el acceso y el contenido de la misma. El usuario podrá listar el contenido de la tarjeta, q se mostrará en forma de árbol, visualizar información sobre los Ids digitales, importar certificados e Ids digitales (admite formatos .CER, .P12 y .PFX), borrar certificados y claves, cambiar el PIN o el PUK de la tarjeta, desbloquear el PIN e incluso verificar la caducidad de los certificados.

GTA trabaja con múltiples lectores y, por consiguiente, con múltiples tarjetas, y admite 3 tipos de formatos hasta el momento: Safesign, FNMT e Incrypto. El correcto funcionamiento de GTA pasa por la previa instalación de los drivers de estos lectores. Sin ellos, no se reconocerá la existencia de éstos ni de las tarjetas insertadas en ellos. Dándose estas condiciones, GTA permite tener conectados varios lectores simultáneamente con su correspondiente tarjeta insertada.



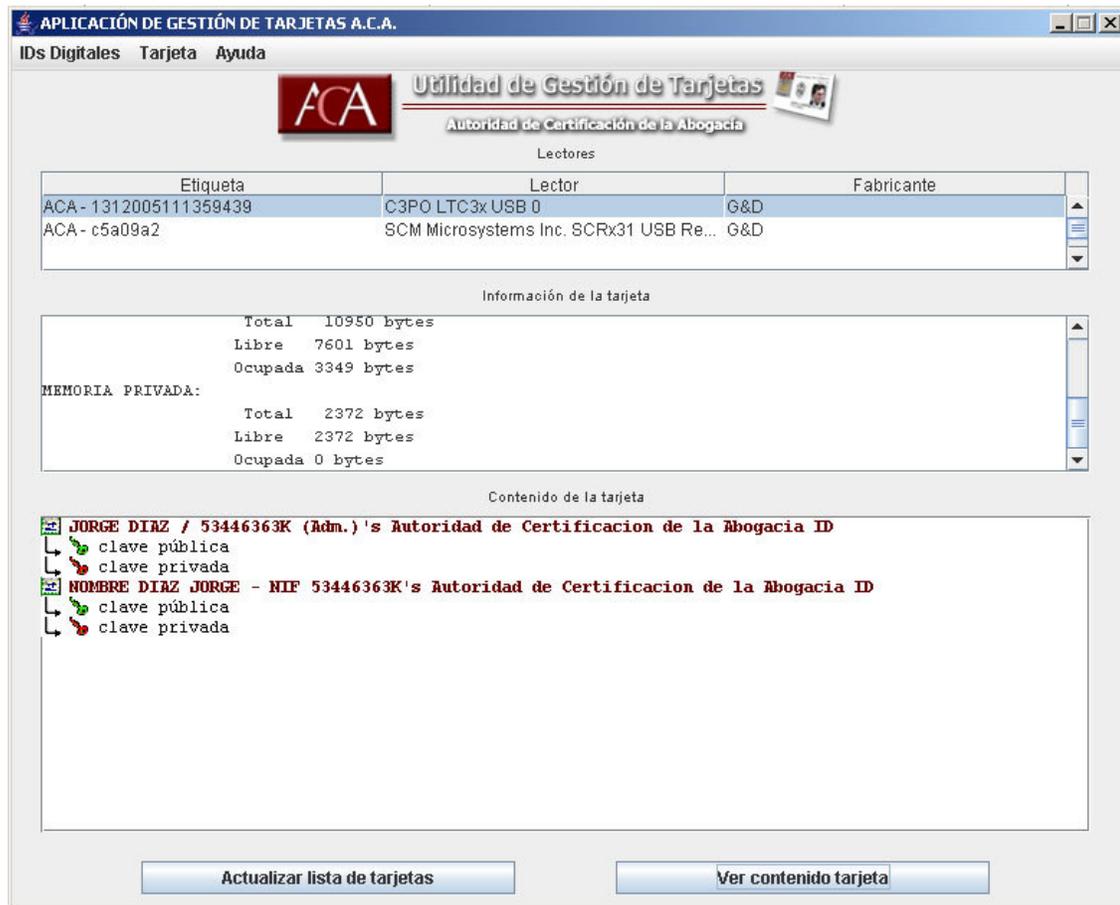
2.4. ABREVIATURAS

ABREVIATURA	DESCRIPCIÓN
CGAE	Consejo General de la Abogacía Española.
ACA	Autoridad de Certificación de la Abogacía
CA	Autoridad certificadora
GTA	Gestor de tarjetas A.C.A.
PIN	Personal Identification Number (Número personal de identificación)
PUK	Personal Unblockig Key (Clave personal de desbloqueo)

3. VENTANA PRINCIPAL:

3.1. DESCRIPCIÓN:

La ventana principal de la aplicación tiene el siguiente aspecto:



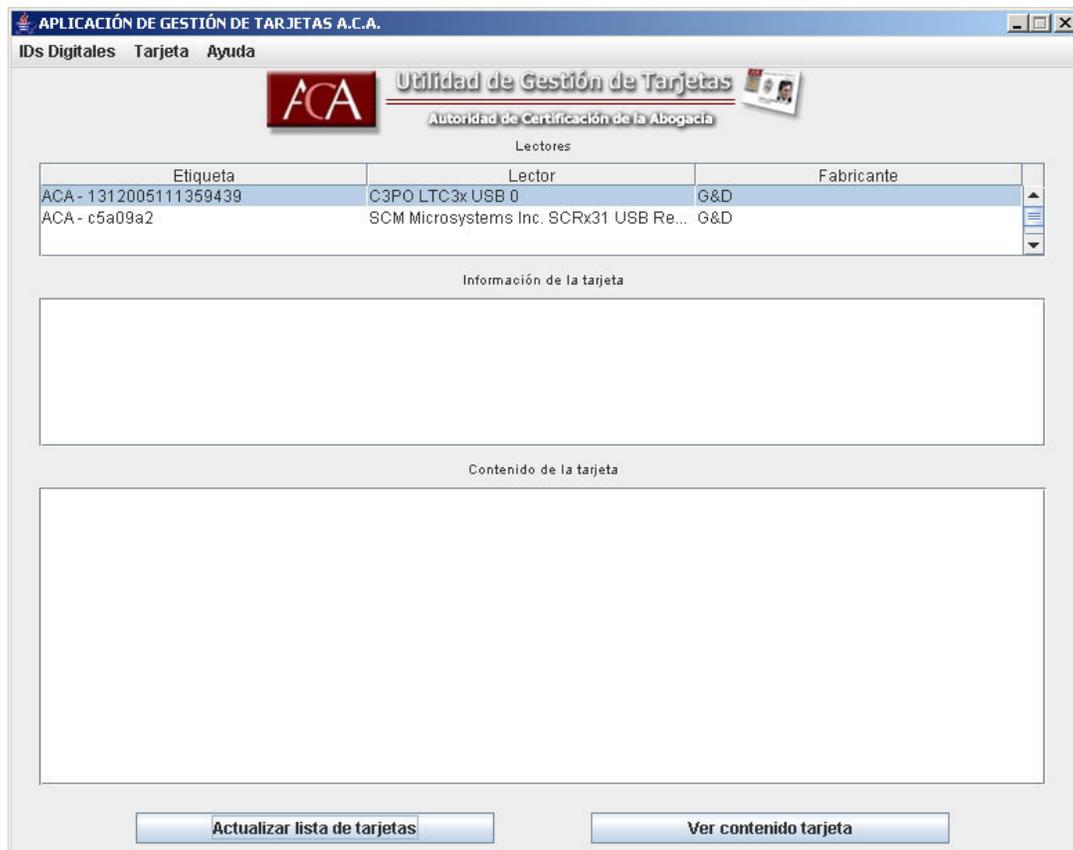
Esta ventana se compone de las siguientes partes diferenciadas:

- Barra de menú: Contiene tres menús principales, IDs Digitales, Tarjeta y Ayuda
- Tabla de lectores: En ella se muestra una lista con los lectores conectados a nuestro ordenador que tienen insertada una tarjeta. La tabla tiene 3 campos:
 - Etiqueta: es un código que identifica a la tarjeta
 - Lector: muestra el nombre del fabricante del lector
 - Fabricante: muestra el nombre del fabricante de la tarjeta insertada en cada uno de los lectores

- Información de la tarjeta: Se trata de un área de texto que mostrará una serie de datos informativos sobre la manufacturación de la tarjeta y su estado actual (número de serie, fabricante, memoria, etc).
- Contenido de la tarjeta: En este panel se muestra un árbol que representa los certificados y las claves contenidos en la tarjeta. En el primer nivel del árbol se nos muestran los certificados y en el segundo las claves, consignando con un icono verde las claves públicas y con uno rojo las claves privadas. Las ramificaciones que surgen del certificado y se unen con las claves nos muestran las dependencias.
- Botones:
 - Actualizar lista tarjetas: al ser pulsado la aplicación comprueba que lectores están conectados en ese instante, y cuáles tienen insertada tarjeta para refrescar el contenido de la tabla de tarjetas
 - Ver contenido tarjetas: Teniendo seleccionado una tarjeta nos permite acceder al contenido de ésta, rellenándose los paneles *Información de la tarjeta* y *Contenido de la tarjeta*.

3.2. OPERACIÓN:

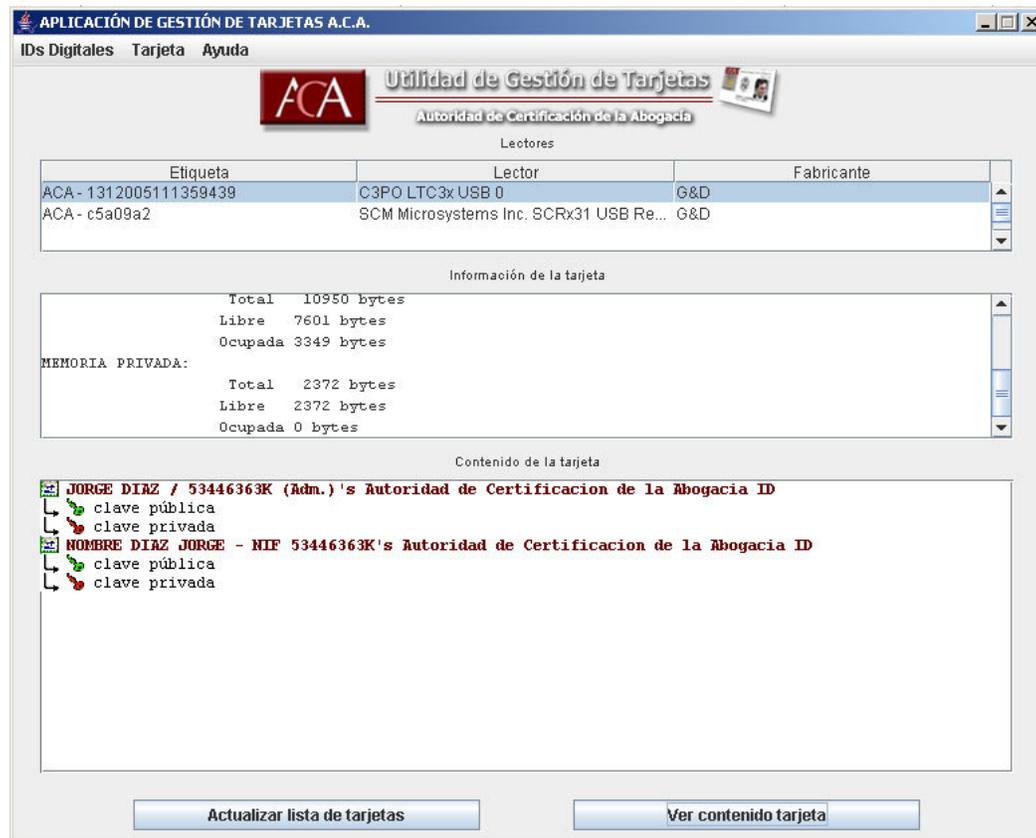
Al entrar en la aplicación el estado de la ventana principal será el siguiente:



Si tenemos insertadas ya la tarjeta o tarjetas con las que queremos trabajar y tenemos seleccionada una tarjeta haremos clic en "Ver contenido tarjeta". En caso contrario haremos clic en en "Actualizar lista tarjetas" y seleccionaremos igualmente la tarjeta para después hacer clic en "Ver contenido de tarjeta". Al pulsar este botón se nos solicitará el PIN de la tarjeta (en las tarjetas que soporta GTA, éste deberá tener entre 4 y 8 caracteres). Si después de tres intentos, no lo introducimos correctamente, el PIN quedará bloqueado, y tendremos que desbloquearlo utilizando el PUK:



Después de introducir el PIN veríamos algo del tipo de lo siguiente:



En nuestro ejemplo, en el panel "Información de la tarjeta" obtenemos la siguiente información:

```
ETIQUETA: ACA - 1312005111359439
FABRICANTE: A.E.T. Europe B.V.
MODELO: 24840D0303000000
NUMERO DE SERIE: 7690484300142321
ESTADO DEL PIN: OK
LONGITUD DEL PIN: Máximo 8carácteres/Mínimo 4 carácteres.
MEMORIA PÚBLICA:
    Total    10950 bytes
    Libre    7601 bytes
    Ocupada  3349 bytes
MEMORIA PRIVADA:
    Total    2372 bytes
    Libre    2372 bytes
    Ocupada  0 bytes
```

En el panel "Contenido de la tarjeta" vemos el árbol de certificados y claves que comentamos antes:



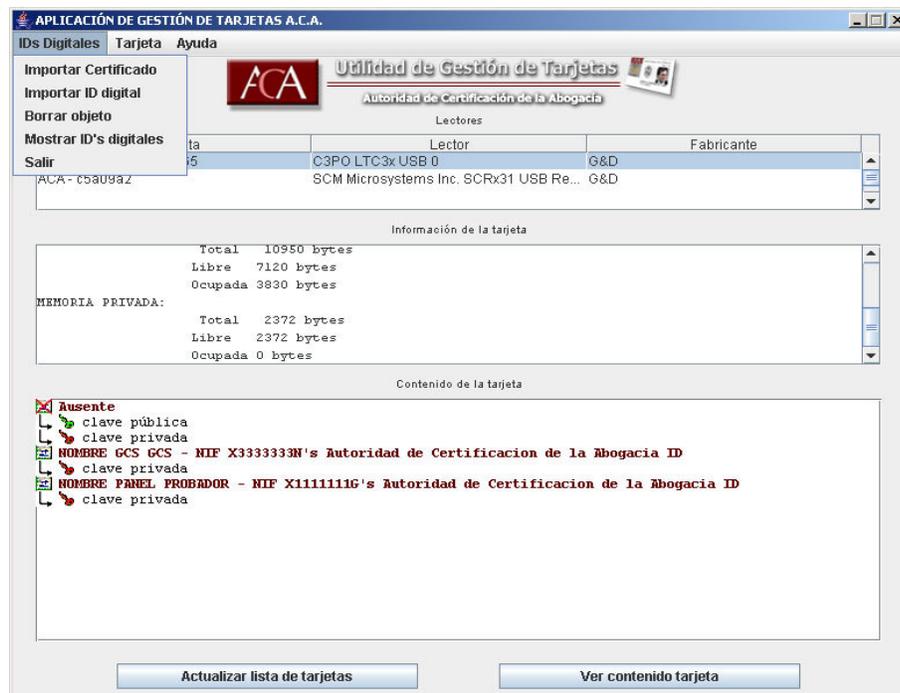
Haciendo clic sobre el icono que representa un certificado veremos como ocultamos/mostramos las claves asociadas a cada certificado (ver arriba).

Haciendo clic sobre el nombre del certificado o de las claves los seleccionamos (vemos que cambian de color), lo cual será necesario, por ejemplo, para borrar un certificado o clave. Si sobre el nombre de un certificado, en lugar de hacer un solo clic, hacemos doble clic, veremos como se nos muestra la ventana de información propia de Windows® que detalla la información del mismo (ver imagen).



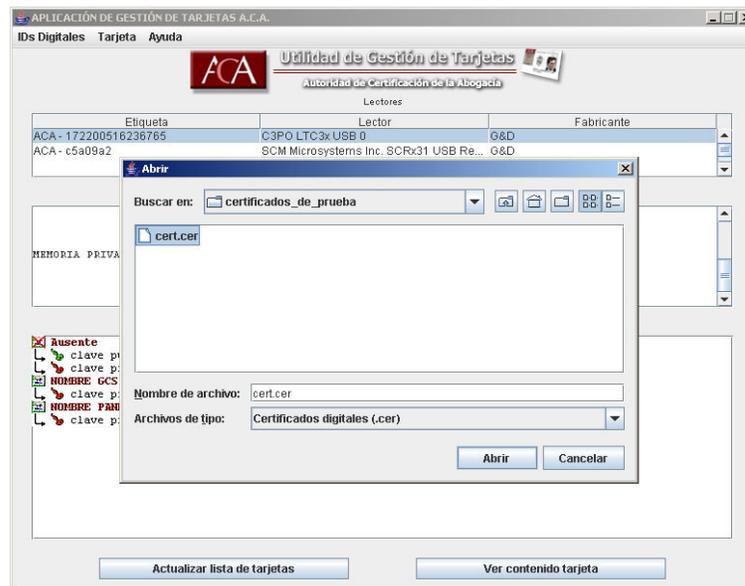
4. MENÚ ID'S DIGITALES:

Es el primer menú de la barra superior y es el que contiene todas las operaciones de gestión del contenido de la tarjeta. Éstas operaciones son: Importar certificado, Importar Id digital, Borrar Objeto y Mostrar Ids digitales. También encontramos aquí la opción de salir de la aplicación.

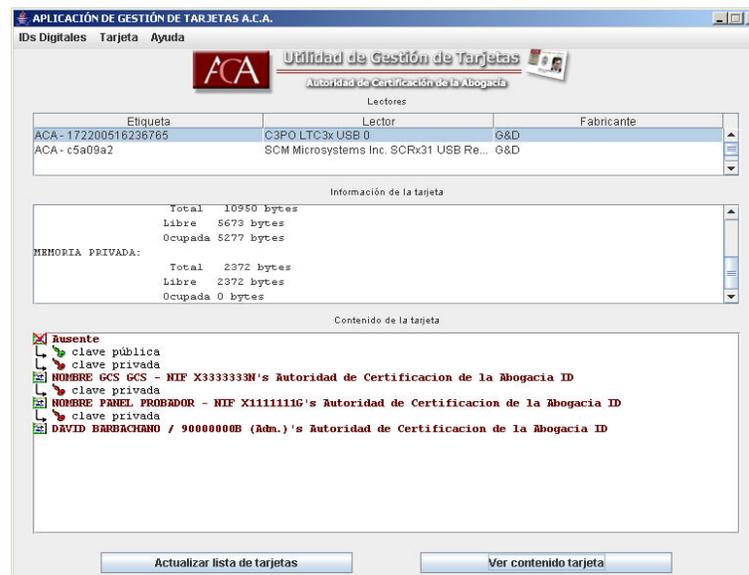


4.1. IMPORTAR CERTIFICADO

Gracias a esta funcionalidad podemos importar certificados (sin claves, sólo certificados) en nuestra tarjeta. Cuando seleccionamos "Importar Certificado" en el menú IDs Digitales se abre una ventana con la que podremos buscar en cualquiera de las unidades de nuestro ordenador un archivo de tipo .CER. Lo seleccionamos y pulsamos "abrir"

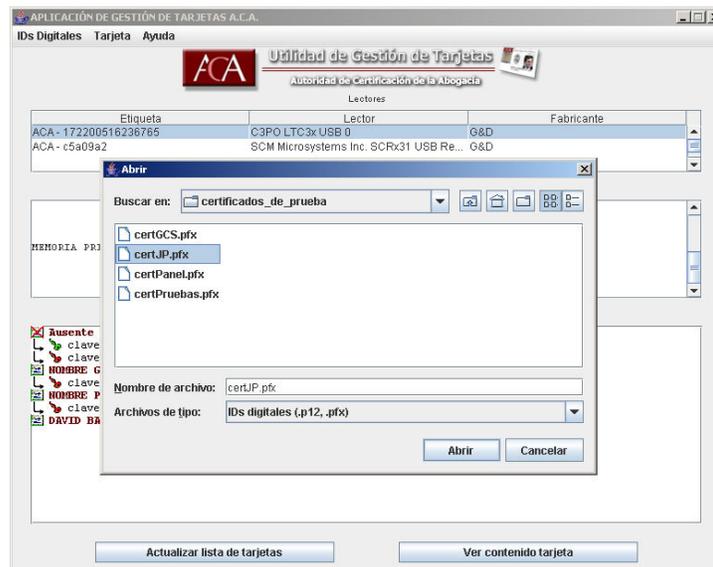


Después de realizar el proceso de importación y actualizar los datos de la tarjeta, aparece el certificado en el árbol de contenido de la tarjeta:

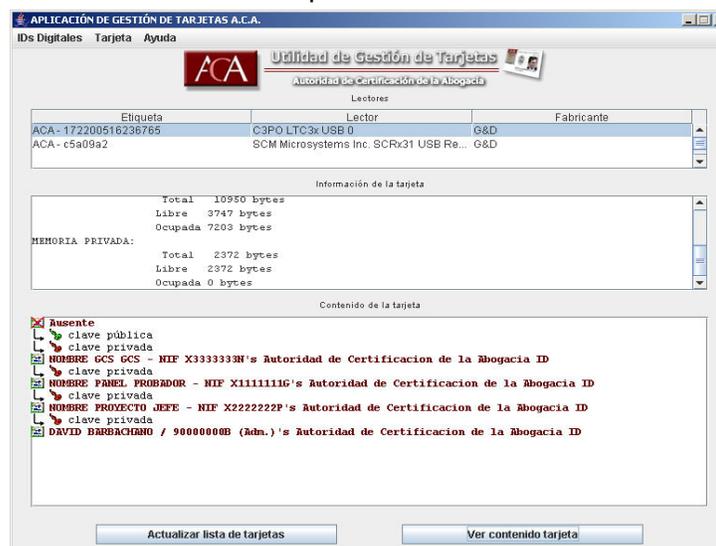


4.2. IMPORTAR ID DIGITAL:

Muy similar a la opción anterior con la salvedad de que lo que importamos en este caso es un archivo del tipo .PFX o .P12, que contiene un certificado con sus correspondientes claves privada y pública (esta última, no tiene por qué estar necesariamente). El proceso es el mismo que en Importar Certificados. Primero buscamos, seleccionamos y abrimos el archivo:

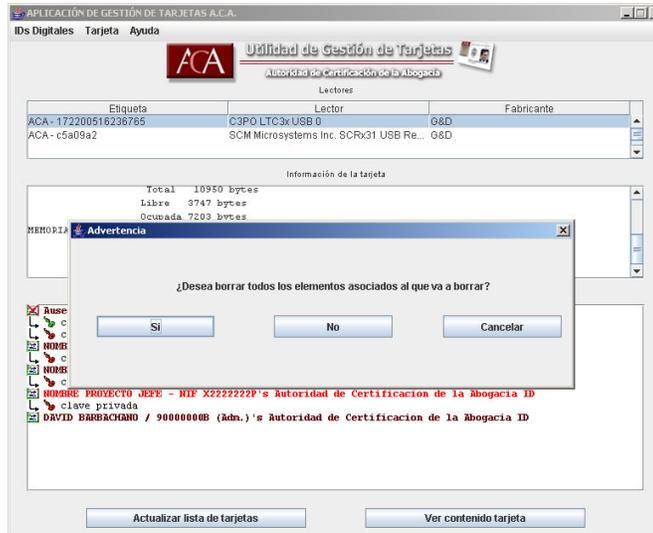


Después de realizar el proceso de importación y actualizar los datos de la tarjeta, vemos como aparece el certificado con su clave privada en el árbol de contenido de la tarjeta:



4.3. BORRAR OBJETO:

Para borrar un objeto debemos seleccionar un elemento en el árbol de contenidos de la tarjeta, ya sea una clave o un certificado. En cualquiera de los dos casos se nos preguntará si deseamos borrar los objetos asociados al que vamos a borrar.



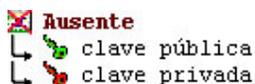
Dependiendo de de lo seleccionado ocurrirá lo siguiente:

- Si hemos seleccionado un certificado, y contestamos que sí, borraremos las claves privada y pública que tenga asociadas (si las tuviera).
- Si hemos seleccionado una clave privada, y contestamos que sí, borraremos el certificado al que pertenece y la clave pública del mismo (si la tuviera).
- Si hemos seleccionado una clave pública, y contestamos que sí, borraremos el certificado al que pertenece y la clave privada del mismo (si la tuviera).

En nuestro ejemplo habíamos seleccionado el certificado, y al responder sí, se eliminó también su clave privada:

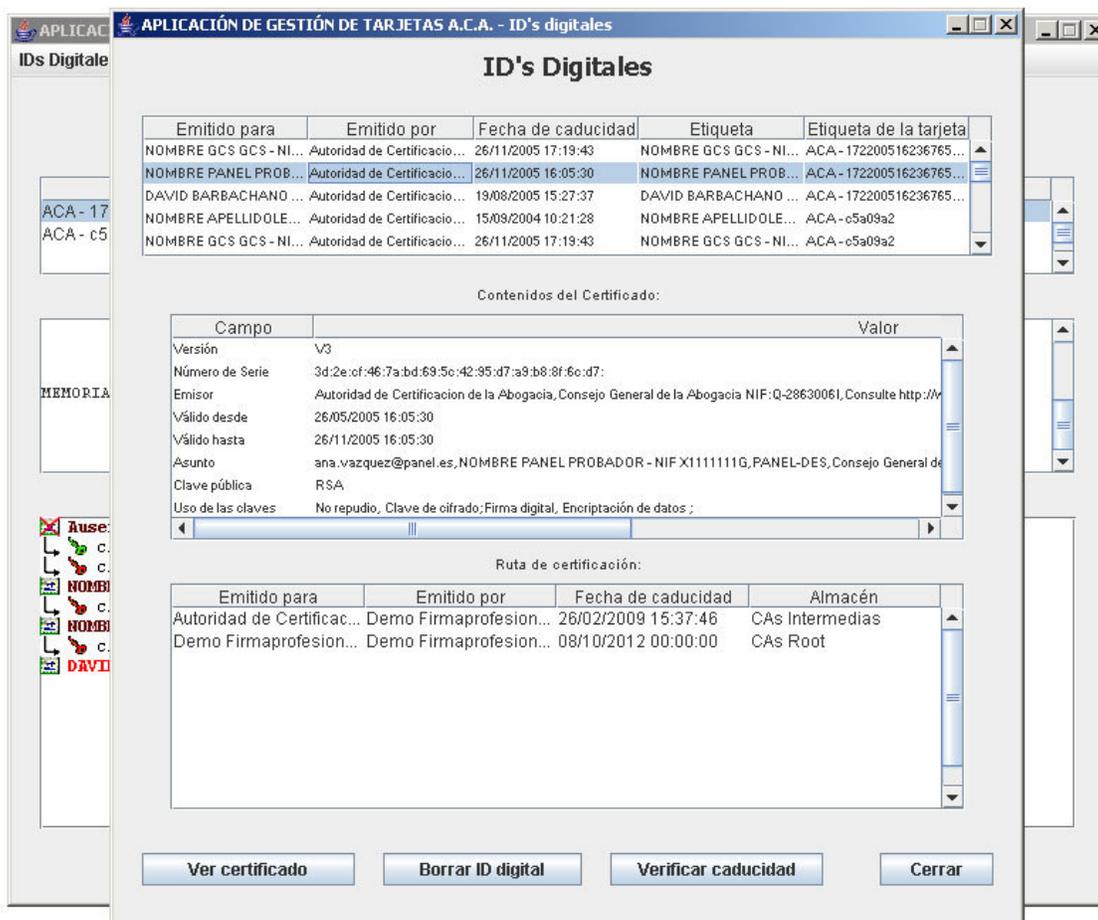


Evidentemente, si decimos que no, se borrará exclusivamente aquel elemento que hayamos seleccionado. Esto, por ejemplo, es lo que ha llevado a un caso como el que ahora mostramos, en el que se hayan dos claves asociadas en la tarjeta, pero su certificado correspondiente no está:



4.4. MOSTRAR IDS DIGITALES:

Desde esta opción accedemos a otra ventana en la que se nos muestran en una sólo lista los Ids digitales de todas las tarjetas insertadas en ese momento. Pulsando sobre cada una de ellas se nos muestra la información que vemos en la siguiente imagen:



APLICACIÓN DE GESTIÓN DE TARJETAS A.C.A. - ID's digitales

ID's Digitales

Emitido para	Emitido por	Fecha de caducidad	Etiqueta	Etiqueta de la tarjeta
NOMBRE GCS GCS - NI...	Autoridad de Certificacio...	26/11/2005 17:19:43	NOMBRE GCS GCS - NI...	ACA - 172200516236765...
NOMBRE PANEL PROB...	Autoridad de Certificacio...	26/11/2005 16:05:30	NOMBRE PANEL PROB...	ACA - 172200516236765...
DAVID BARBACHANO ...	Autoridad de Certificacio...	19/08/2005 15:27:37	DAVID BARBACHANO ...	ACA - 172200516236765...
NOMBRE APELLIDOLE...	Autoridad de Certificacio...	15/09/2004 10:21:28	NOMBRE APELLIDOLE...	ACA - c5a09a2
NOMBRE GCS GCS - NI...	Autoridad de Certificacio...	26/11/2005 17:19:43	NOMBRE GCS GCS - NI...	ACA - c5a09a2

Contenidos del Certificado:

Campo	Valor
Versión	v3
Número de Serie	3d:2e:cf:46:7a:bd:69:5c:42:95:d7:a9:b8:8f:6c:d7:
Emisor	Autoridad de Certificación de la Abogacía, Consejo General de la Abogacía NIF:Q-28630061, Consulte http://www.abogacia.es
Válido desde	26/05/2005 16:05:30
Válido hasta	26/11/2005 16:05:30
Asunto	ana.vazquez@panel.es,NOMBRE PANEL PROBADOR - NIF X1111111G,PANEL-DES,Consejo General de la Abogacía
Clave pública	RSA
Uso de las claves	No repudio, Clave de cifrado;Firma digital, Encriptación de datos ;

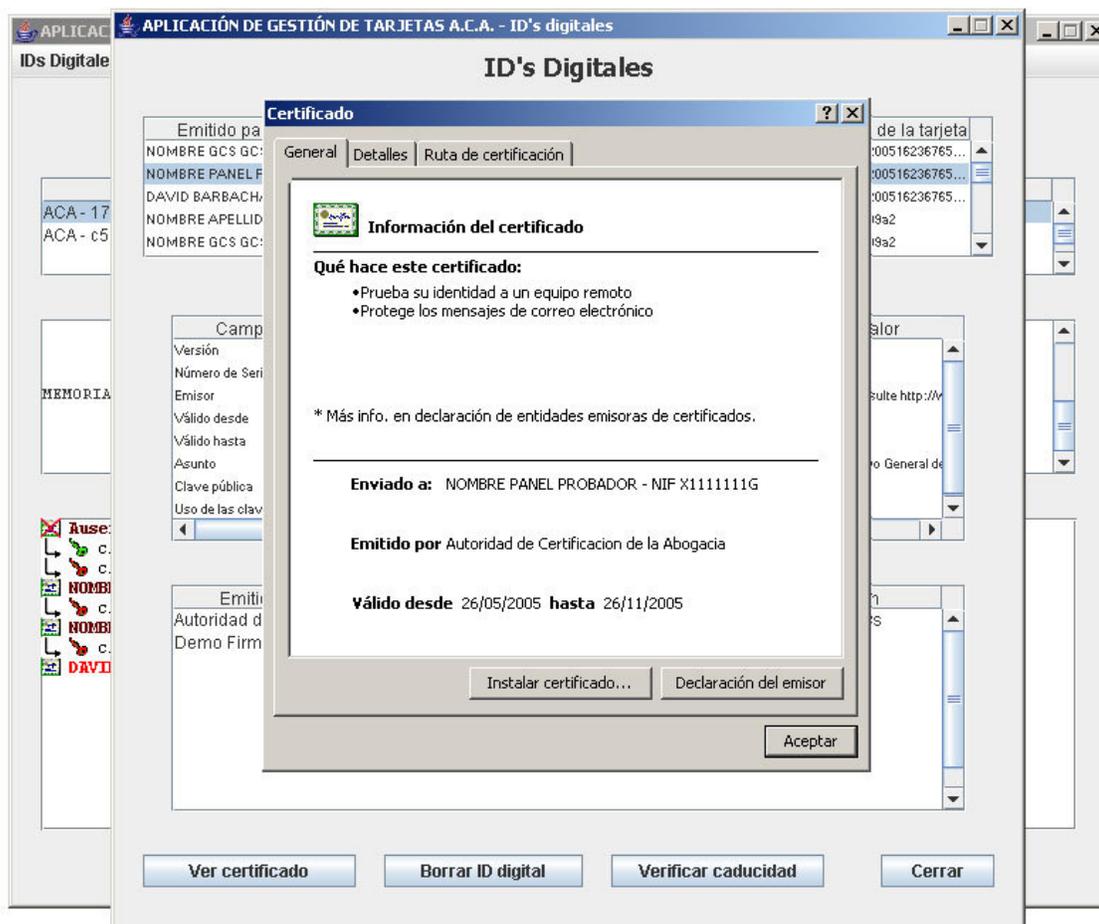
Ruta de certificación:

Emitido para	Emitido por	Fecha de caducidad	Almacén
Autoridad de Certificac...	Demo Firmaprofesion...	26/02/2009 15:37:46	CAs Intermedias
Demo Firmaprofesion...	Demo Firmaprofesion...	08/10/2012 00:00:00	CAs Root

Como vemos, tenemos información referente al certificado (versión, número de serie, emisor, etc) y a la ruta de certificación del mismo (CA Intermedia y CA raíz).

Además desde la ventana de Ids digitales podemos se nos ofrece la posibilidad de realizar algunas acciones desde los botones de la parte inferior, como:

- **Ver certificado:** Se nos muestra la ventana de Windows® de información del certificado, como cuando hacemos doble click sobre un certificado en la ventana principal de la aplicación.



- **Borrar ID digital:** Podemos desde aquí borrar un certificado junto con sus claves (si las tiene) de cualquiera de las tarjetas insertadas. Para borrar desde esta ventana es necesario introducir el PIN de la tarjeta que contiene el elemento a borrar. Podemos constatar como, al borrar el certificado, se actualiza el estado de la tarjeta en la ventana principal.
- **Verificar caducidad:** Pulsando este botón aparecerá una ventana de aviso por cada uno de los certificados que, o bien está caducado, o su fecha de caducidad está próxima.



5. MENÚ TARJETA:

Este es el menú desde que podremos acceder a las opciones que afectan al acceso a la tarjeta. Se trata de las siguientes:

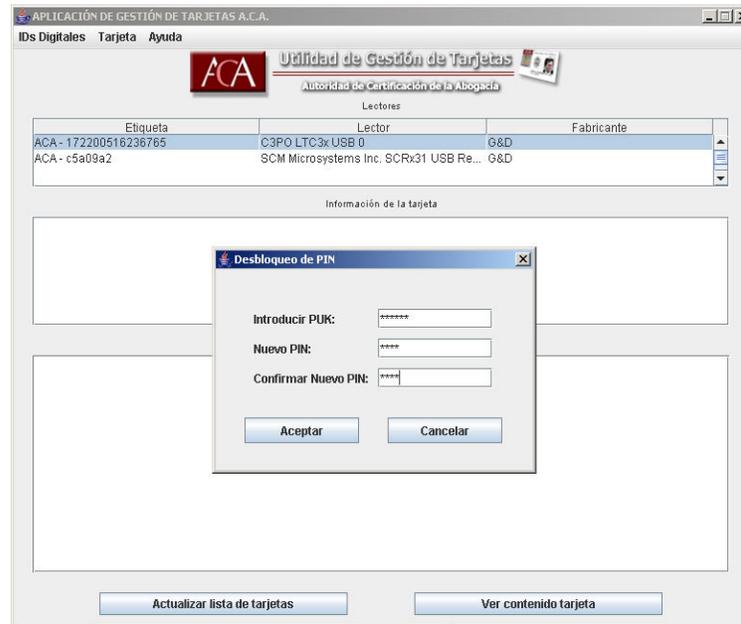
- Desbloquear PIN
- Cambiar PIN
- Cambiar PUK

5.1. DESBLOQUEAR PIN:

Como comentamos en el punto [3.2](#) Al pulsar este botón "*Ver contenido de tarjeta*" se nos solicitará el PIN de la tarjeta (en las que soporta GTA, éste deberá tener entre 4 y 8 caracteres) y si después de tres intentos no lo introducimos correctamente, el PIN quedará bloqueado. Para desbloquearlo utilizamos esta opción.

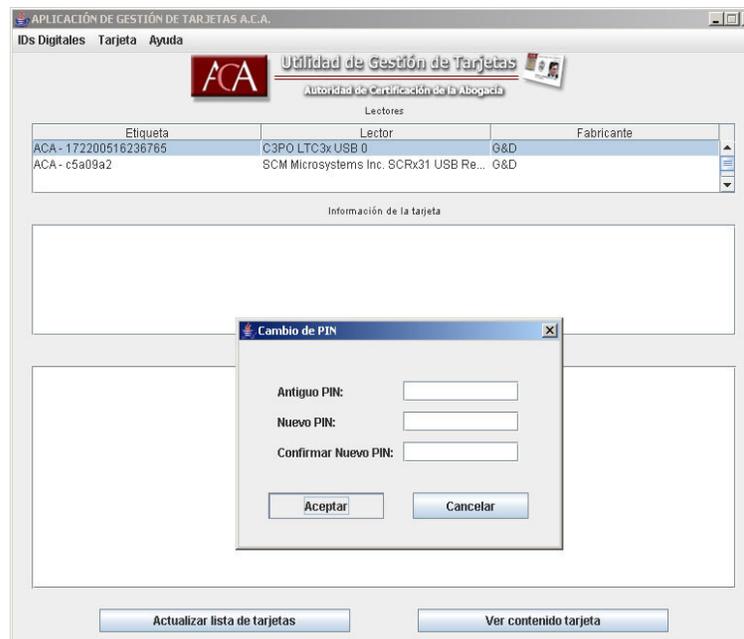
Para poder desbloquear el PIN es necesario conocer el PUK de la tarjeta. Además del PUK, tenemos que introducir el nuevo PIN por duplicado para confirmar que no nos hemos equivocado al escribirlo. Por razones de seguridad, no se verá lo que escribimos (vemos el símbolo "*" en su lugar), de manera que nadie más pueda conocer éstos datos.

Importante: si introducimos el PUK de forma errónea 3 veces, éste quedará bloqueado y, por consiguiente, la tarjeta quedará inutilizada.



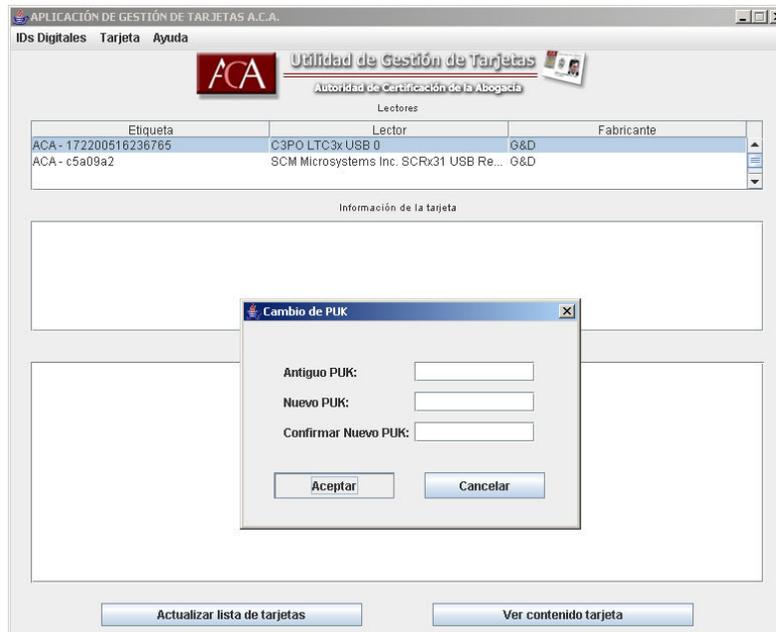
5.2. CAMBIAR PIN:

Para cambiar el PIN de la tarjeta necesitamos introducir el antiguo PIN y el nuevo PIN por duplicado. Si introducimos el PIN de forma errónea 3 veces, éste quedará bloqueado y tendremos que desbloquearlo para recuperar el acceso a la tarjeta.



5.3. CAMBIAR PUK:

Para cambiar el PUK de la tarjeta necesitamos introducir el antiguo PUK y el nuevo PUK por duplicado. Si introducimos el PUK de forma errónea 3 veces, éste quedará bloqueado y, por consiguiente, la tarjeta quedará inutilizada.



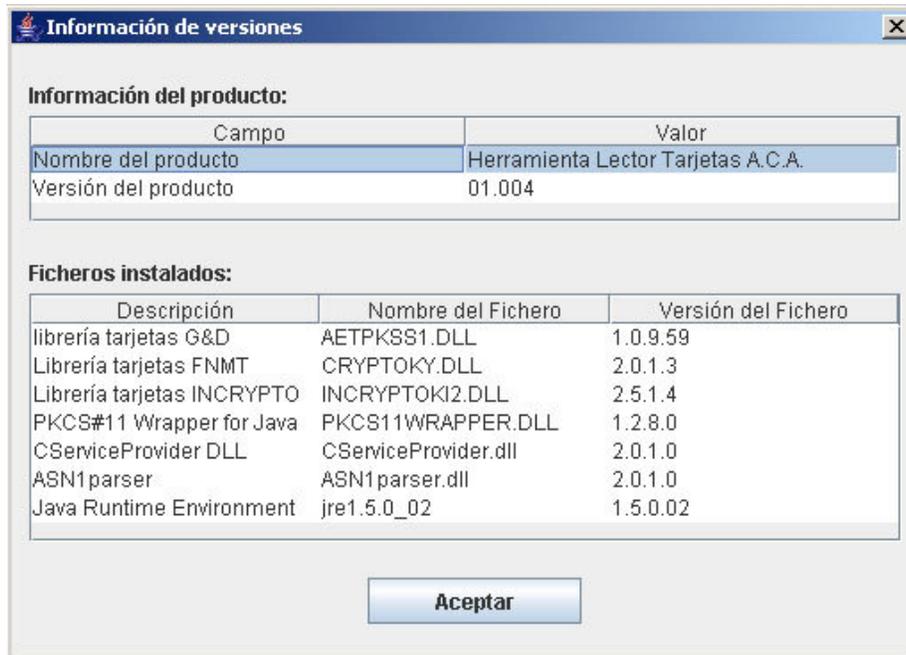
6. MENÚ AYUDA:

En esta sección encontramos las típicas opciones que nos dan información sobre la aplicación. Son dos:

- Información de las versiones
- Acerca de...

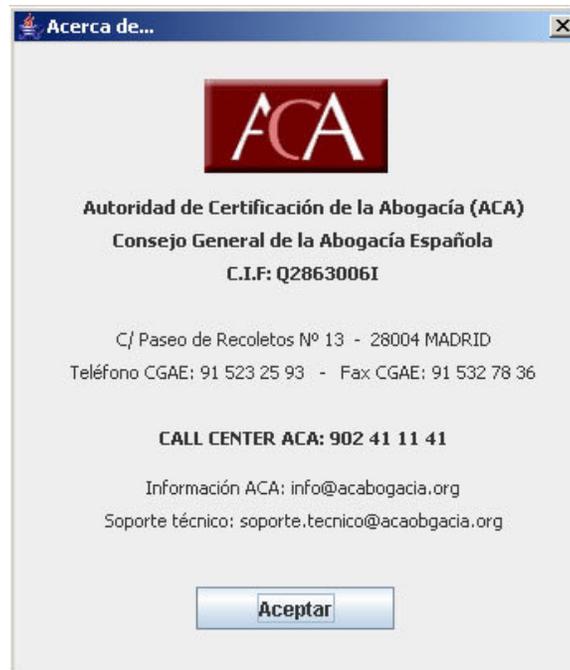
6.1. INFORMACIÓN DE LAS VERSIONES:

Al seleccionar esta opción del menú Ayuda se nos muestra la información referente a la versión de la aplicación y de los archivos de los que depende nuestra aplicación. GTA depende de las librerías propias de los fabricantes de las tarjetas, y de otras necesarias para establecer la comunicación con éstas. Éstos datos son susceptibles de ser actualizados en futuras versiones de GTA si se cambia a futuras versiones de dichas librerías.



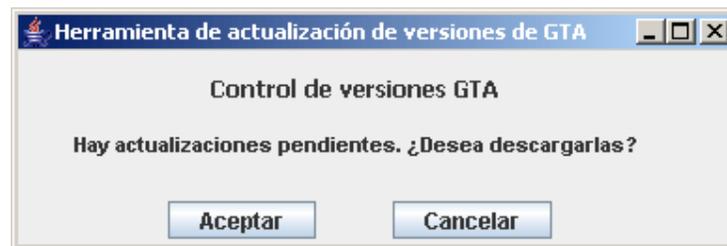
6.2. ACERCA DE:

Esta opción muestra información sobre el distribuidor de la aplicación, y los datos de contacto (dirección, teléfono y direcciones de correo electrónico de información y soporte).

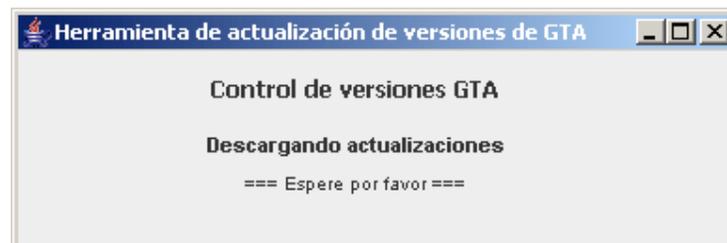


7. ACTUALIZACIÓN AUTOMÁTICA:

GTA es capaz de actualizarse de forma automática. Para ello realiza una comprobación al arrancarse la aplicación, conectándose al servidor de versiones, para ver la posible existencia de una nueva versión, en caso de que se hallen versiones superiores a la que tenemos instalada, aparecerá la siguiente ventana:



Si pulsamos "Cancelar" arrancaremos directamente GTA, pero si pulsamos "Aceptar" comenzará el proceso de descarga de las actualizaciones. La ventana de proceso tiene el siguiente aspecto:



El proceso puede tomar varios minutos, dependiendo de la magnitud de la actualización. Cuando termine el proceso de descarga e instalación, puede ocurrir una de dos cosas: O bien se arranca directamente GTA, en el caso de que no se hayan incluido nuevos archivos, o bien se nos solicitará reanunciar la aplicación, para que los nuevos archivos entren en ejecución:





Manual de usuario GTA.



		<i>Versión: 1.2</i>
--	--	----------------------------