

Protocolo de comunicación con la IES.

Dirección General de Operaciones de Banca Central
Dirección de Sistemas Operativos y de Pagos
Gerencia de Informática

Agosto de 2003¹

Resumen

Este documento muestra el protocolo de comunicación de la IES, incluyendo los mapas de mensajes.

Índice

1. Formato	2
2. Mensajes firmados	4
3. Mapas de mensajes para la IES	7
4. Formato de los mensajes del protocolo	12
5. Comentarios	18

¹Última revisión: Junio de 2005.
Comentarios y sugerencias: Soporte IES
ies@banxico.org.mx

El protocolo actual utiliza mensajes que constan de dos partes: encabezado y cuerpo. En el encabezado se especifica el tipo de mensaje que se quiere intercambiar junto con su longitud, mientras que en el cuerpo se encuentra la información deseada.



Tanto el cuerpo como el encabezado de cada mensaje se construyen con los tipos de datos básicos de los lenguajes de programación: `char`, `int`, `short`, `string`.

1. Formato

El formato de un mensaje es una secuencia de tipos de datos básicos. Para crear estas secuencias a cada tipo de datos se la ha asignado un símbolo, como se muestra en la siguiente tabla:

Tipo de dato	Símbolo	Tamaño en bytes
char	%c	1
short	%d	2
int	%l	4
string	%s	Variable, terminación carácter nulo

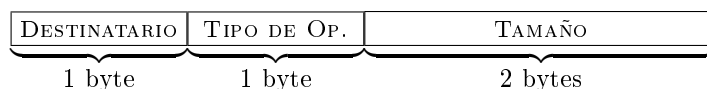
Debido a que no todos los sistemas interpretan los tipos de datos `int` y `short` de la misma forma (algunos utilizan el formato “LITTLE ENDIAN”, mientras que otros utilizan “BIG ENDIAN”), se pide que estos tipos de datos viajen en formato de red, para que cualquier sistema pueda interpretarlos correctamente.

A continuación se muestra un ejemplo de la interpretación de este formato:

FORMATO	INTERPRETACIÓN
%l %l %s	En una cadena de bytes viajan 3 datos, el primero se puede obtener a partir de los bytes 1 al 4, el segundo a partir de los bytes 5 al 8 y, finalmente, el tercero a partir del byte 9 y hasta que encuentre un caracter nulo.
%c %d %l %sn(%c %d %l %s)	Este formato contiene un número variable de datos. El primer dato ocupa un byte, el segundo ocupa 2 bytes, el tercero ocupa 4 bytes, el cuarto es una cadena con terminación en caracter nulo y después hay una serie de "n" elementos (este valor de "n" ocupa 4 bytes y debe viajar en formato de red) de los tipos descritos dentro de los paréntesis, es decir, hay "n" elementos de un byte, "n" elementos de dos bytes, "n" elementos de 4 bytes y por último, "n" cadenas de caracteres con terminación el caracter nulo.

El encabezado de un mensaje tiene una longitud fija de 4 bytes y tiene la siguiente forma:

ENCABEZADO DEL MENSAJE



- El formato del encabezado del mensaje es: %c %c %d.
- DESTINATARIO : Todo cliente que se conecte con una Agencia Registradora (AR) de la IES deberá establecer el valor de este campo igual a CERO. En el caso de los servidores que se conectan con la Agencia Registradora Central (ARC) deberán establecer este valor de acuerdo a los lineamientos siguientes:
 1. Si el servidor es el originador de la solicitud hacia la ARC, el valor de este campo será de CERO (por ejemplo, el mensaje RevCrt).
 2. Si la ARC origina la solicitud hacia el servidor entonces el valor de este campo se deberá mantener de acuerdo al asignado por la ARC, ya que de esta forma se identifica al cliente que originó la petición (por ejemplo, el mensaje PideCrtNvoFmt, que la ARC le manda a una AR reconocida para solicitarle un certificado y, que previamente dicha AR se conectó e identificó con la misma ARC).

- TIPO DE OPERACIÓN : Operación que se desea realizar (1 byte). De esta forma tenemos a lo más 256 operaciones distintas para definir.
- TAMAÑO : Longitud en bytes del cuerpo del mensaje, sin incluir el encabezado (2 bytes).

El cuerpo de un mensaje es un arreglo de bytes de longitud variable. Su construcción se efectúa a partir de los tipos de datos ya mencionados y , evidentemente, el cuerpo del mensaje depende del tipo de operación que se indique en el encabezado.

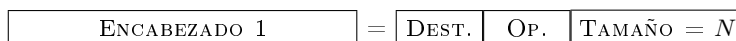
2. Mensajes firmados

Dentro del intercambio de mensajes con la IES (ARC y AR de Banxico) existen algunos mensajes que deben ir firmados. La diferencia en el formato del mensaje firmado con el formato del mensaje sin firmar es que al primero se le debe añadir un “%I” al inicio del cuerpo, el cual indica el tamaño de la firma. La construcción de este tipo de mensajes se resume a continuación:

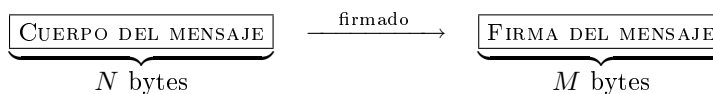
1. Construir el encabezado del mensaje que se desea firmar. Además construir el cuerpo del mensaje y depositarlo en un buffer.



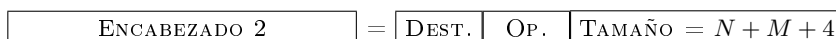
En donde



2. Firmar el buffer del *cuerpo del mensaje* creado en el paso 1, pasarlo a una cadena (%s) en formato Base-64 y obtener su longitud **sin considerar el caracter terminador nulo de la misma**.



3. Construir el encabezado del mensaje firmado. Al calcular el tamaño del nuevo cuerpo, se debe tomar en cuenta que el campo para colocar el tamaño de la firma ocupa 4 bytes y se debe sumar además el tamaño de la misma firma (sin considerar el caracter terminador nulo).



4. Construir el cuerpo del mensaje firmado. La diferencia de este cuerpo con el del mensaje sin firmar es que al cuerpo del mensaje firmado se le añade al inicio el tamaño de la firma y se le agrega al final la firma realizada en el paso 2, en formato Base-64 y **sin terminar dicha firma con el caracter nulo.**



OBSERVACIÓN: El formato del mensaje firmado difiere del formato del mensaje a firmar en un “%l” al inicio; además el cuerpo entre estos dos mensajes, difiere en un entero al inicio y un arreglo de bytes al final del mismo. Es importante notar que el arreglo de bytes correspondiente con la firma, no se expresa en el formato del mensaje firmado. Como ejemplo supongamos que el formato de un mensaje, el cual llamaremos mensaje A, es “%l%d%s” (un entero de 4 bytes, un entero de 2 bytes y una cadena de caracteres), el formato correspondiente del mensaje firmado es “%l%l%d%s” (en lugar de “%l%l%d%s%s”) y la información contenida en el cuerpo del mensaje es un entero de 4 bytes que representa la firma hecha sobre el mensaje A, el entero de cuatro bytes de A, el entero de 2 bytes del mensaje A, la cadena de caracteres del mensaje A y, finalmente, la cadena de caracteres que corresponde a la firma, pero quitándole el caracter nulo del final.

Un ejemplo práctico sigue a continuación:

Supóngase que se va a conectar con un certificado cuyo número de serie es **00000100200400000003**. El buffer armado para firmar consta sólomente de la cadena con el número de serie, por lo que en hexadecimal, se representaría así:

30 30 30 30 30 31 30 30 32 30 30 34 30 30 30 30 30 30 30 33 00

Nótese que este mensaje sí se termina con el nulo (caracter 00). Enseguida se firma con la clave privada asociada a dicho certificado y se convierte el resultado a base 64. Si la firma resultante fuera la siguiente,

MoCOcTHJL6tSX9hUcqqZXXC/7+TpVb6WzBeSZ72vqFv6fPdZvdPQT++m2TyFEVX
i0vvHE+CkxYiVvnT6mH+0g+9EXv7Sm1DZEG0teGkiwG9cA2apyxKk/g4QPMOCBN
rwGF7JK4Fz5f/Jd42vqTBDfUIafwJEqh361v27jrhBvTs=

entonces la longitud de la firma es 172, que en hexadecimal se representaría (usando 4 bytes) como:

00 00 00 ac

El cuerpo del mensaje firmado resultante, en hexadecimal, sería el siguiente:

```

00 00 00 ac 30 30 30 30 30 31 30 30 32 30 30 34 30 30 30 30 30
30 30 30 33 00 4d 6f 43 30 63 54 48 4a 4c 36 74 53 58 39 68 55 63
71 71 5a 58 58 43 2f 37 2b 54 70 56 62 36 57 7a 42 65 53 5a 37 32
76 71 46 76 36 66 50 64 5a 76 64 50 51 54 2b 2b 6d 32 54 79 46 45
56 58 69 4f 76 76 48 45 2b 43 6b 78 59 69 56 76 6e 54 36 6d 48 2b
4f 67 2b 39 45 58 76 37 53 6d 31 44 5a 45 47 30 74 65 47 4b 69 77
47 39 63 41 32 61 70 79 78 4b 6b 2f 67 34 51 50 4d 30 43 42 4e 72
77 47 46 37 4a 4b 34 46 7a 35 66 2f 4a 64 34 32 76 71 54 42 44 46
75 49 61 66 77 4a 45 71 68 33 36 6c 76 32 37 6a 72 68 42 76 54 73
3d

```

Nótese que el mensaje termina en 3d, no en 00, ya que el carácter nulo de la firma no se manda.

El cuerpo del mensaje tiene 198 bytes de longitud, constituido por los 4 bytes de la longitud de la firma, los 22 bytes del cuerpo del mensaje original (sin firmar) y los 172 bytes correspondientes a la firma. Este valor debe quedar reflejado en el encabezado del mensaje resultante.

Para la verificación de la firma de uno de estos mensajes se procede del siguiente modo:

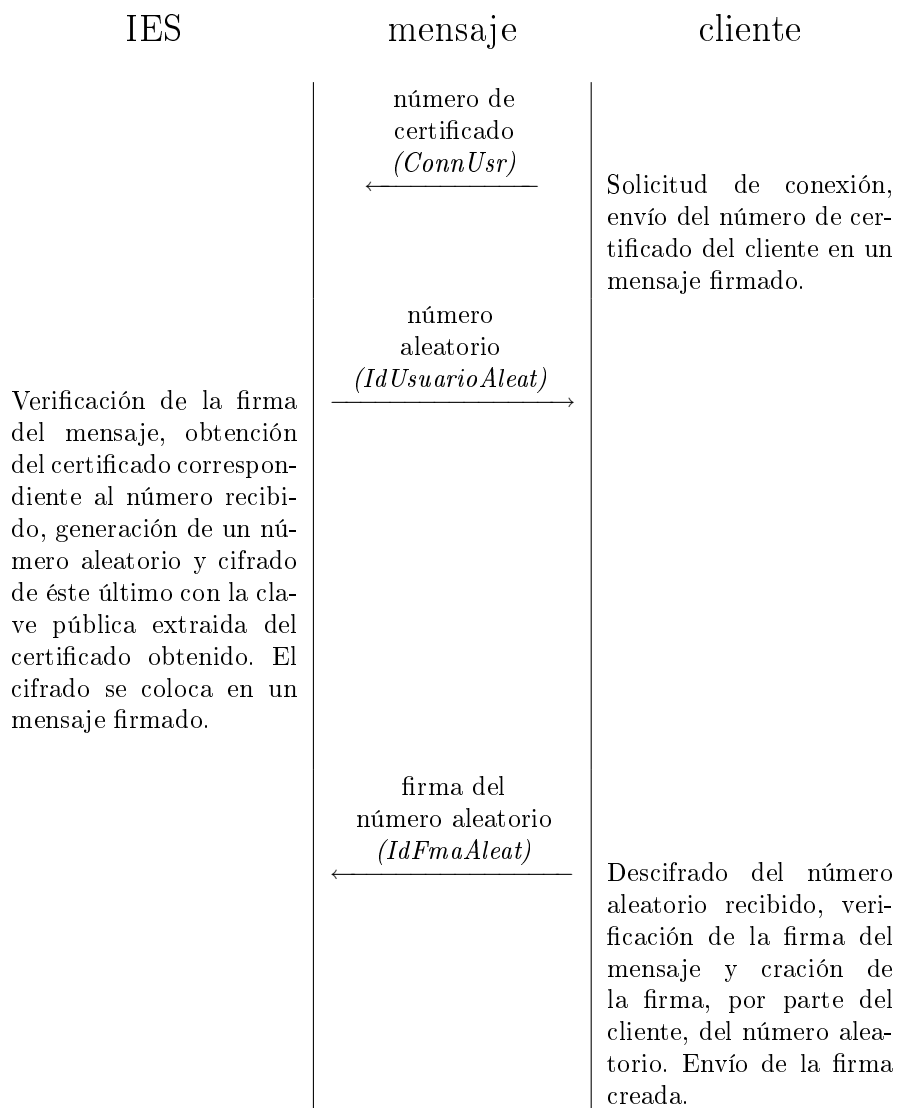
1. Extraer del mensaje firmado, el tamaño de la firma y el buffer correspondiente a la firma².
2. Construir el cuerpo del mensaje correspondiente al mensaje sin firma.
3. Verificar el mensaje obtenido en el paso 2 contra la firma obtenida en el paso 1.

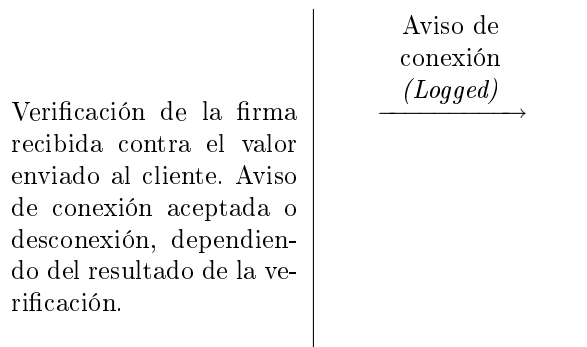
²Esto se puede hacer por diferencia de longitudes entre la del cuerpo y la correspondiente a la firma, recordando que esta última no está terminada con un carácter nulo

3. Mapas de mensajes para la IES

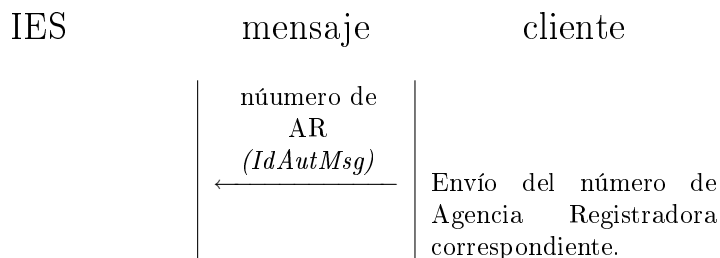
A continuación se bosqueja el esquema de conexión a la IES.

Conexión de un cliente con la IES (ARC o AR).

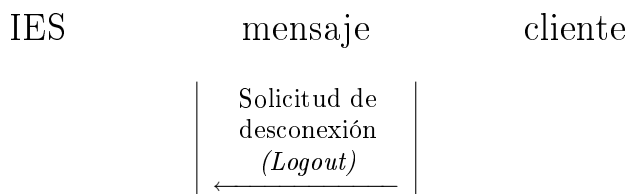




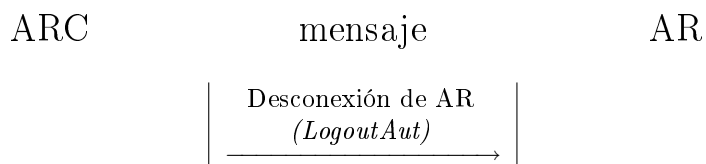
En caso de que una AR solicite conexión a la ARC se deberá enviar adicionalmente el mensaje siguiente.



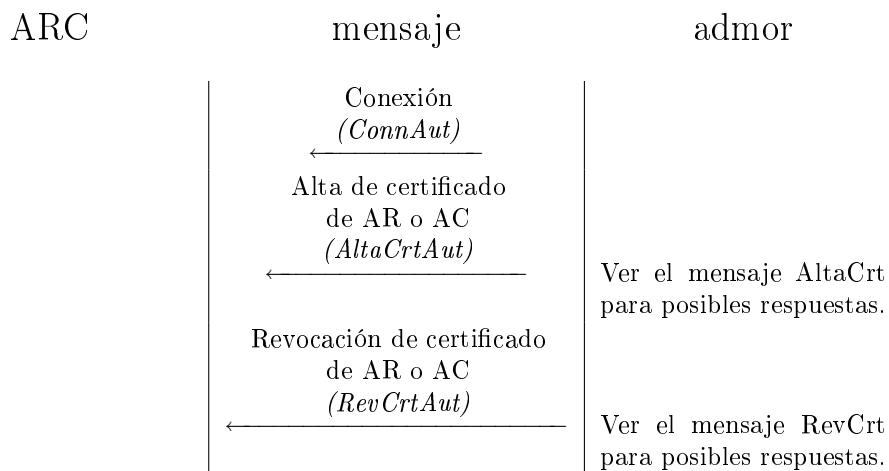
Desconexión de un cliente de la ARC o AR.



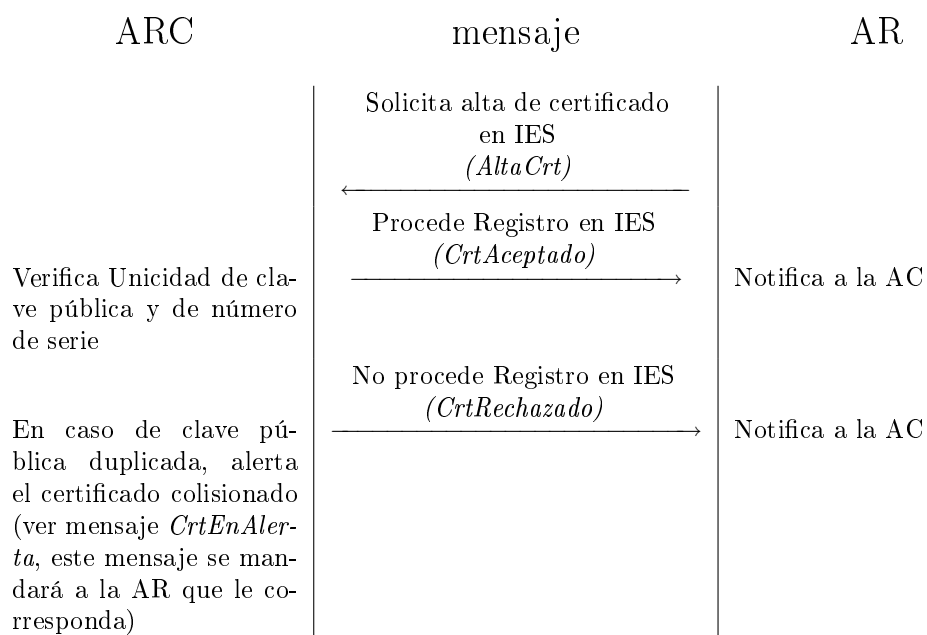
Desconexión de una AR por petición de la ARC.



Mensajes de administración local.

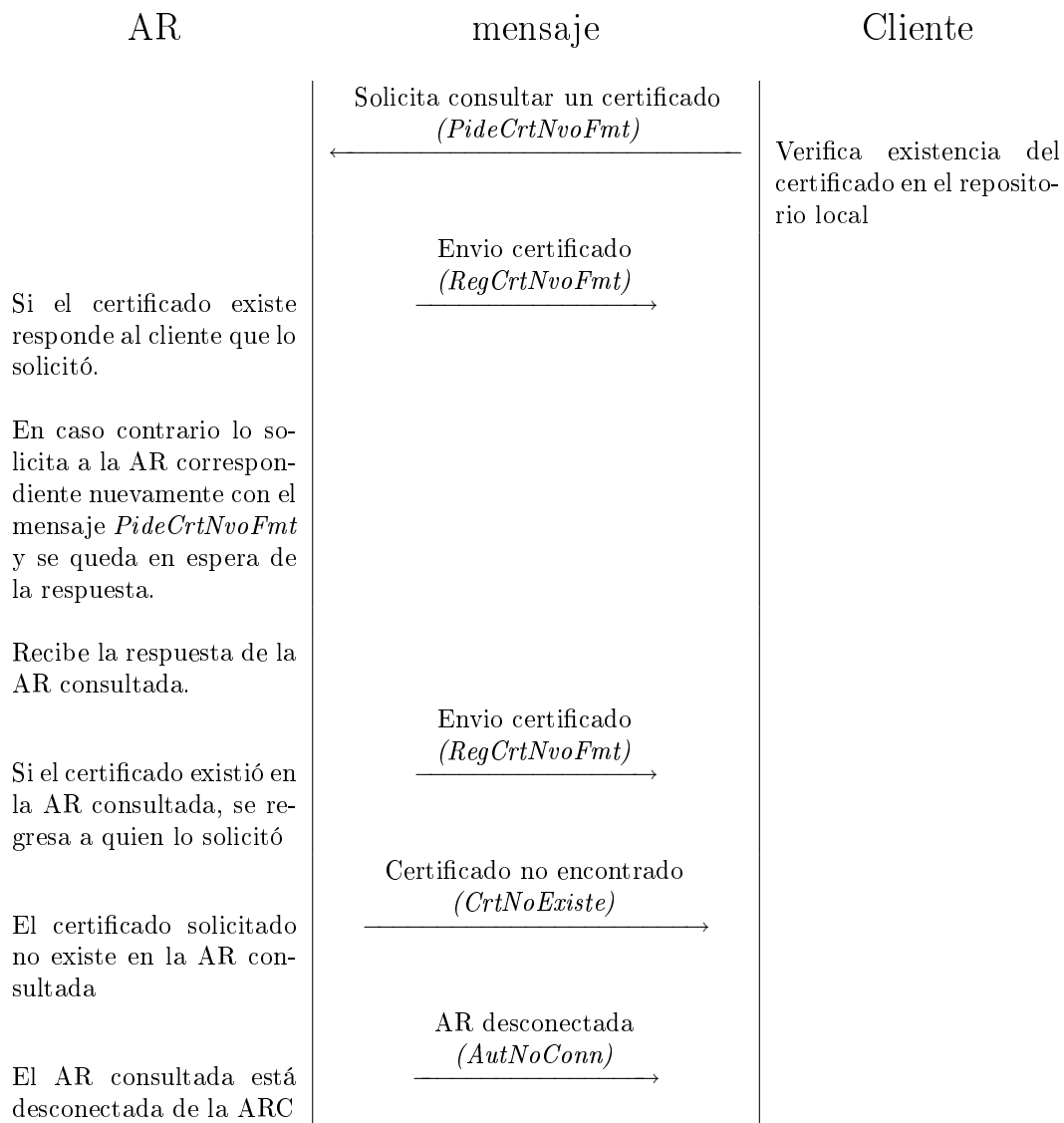


Alta de certificado: Mensajes de la AR a la ARC³.



³Para los servidores en Banxico, estos mismos mensajes aplican para dar de alta un certificado en la AR desde la AC.

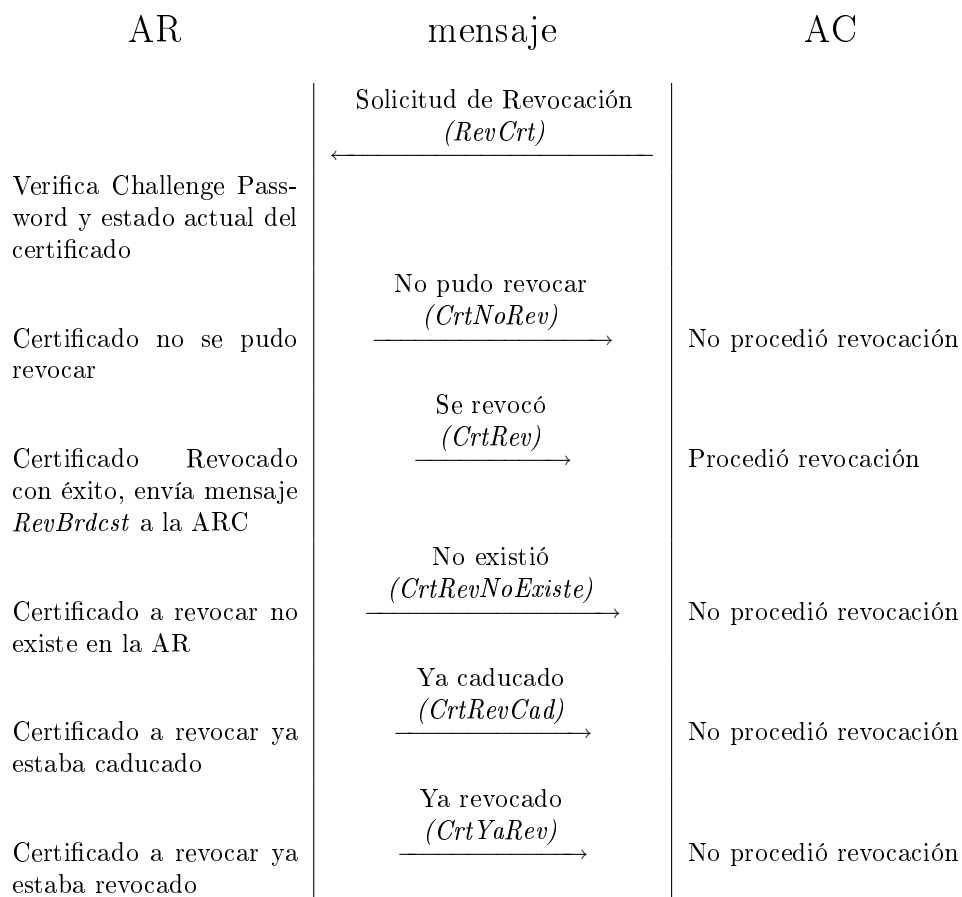
Consulta de certificado: Mensajes de la AR a la ARC Banxico⁴.



NOTA: El mapa de mensajes para el *VerifCrtCorto* es análogo al *RegCrtNvoFmt*, siendo la respuesta con el certificado *RegCrtCorto* en lugar de *RegCrtNvoFmt*.

⁴Estos mensajes aplican también para los clientes conectados a los servidores AR de Banxico y que solicitan certificados.

Revocación de un certificado: Mensajes entre la AC y la AR⁵



⁵Únicamente aplican para las ARs del Banco de México

Revocación de un certificado: Mensajes entre la AR y la ARC.



4. Formato de los mensajes del protocolo

En la siguiente tabla se muestran los mensajes enviados por los clientes a la IES (ARC y AR de Banxico).

No.	Nombre	Formato	Descripción	Firma	Posibles respuestas
0	LOGOUT		Fin de conexión.	no	Desconexión.
16	ConnUsr	%l %s	Solicitud de conexión.	si	OprNoPermit, IdUsuarioAleat, Desconexión.
18	ConnAut	%l %s	Solicitud de conexión.	si	OprNoPermit, IdUsuarioAleat, Desconexión.
19	RevBrdcst	%l %l %s	Aviso de revocación.	si	
90	AltaCrt	%l %s %s	Solicitud de alta de certificado.	si	CrtAceptado, CrtRechazado.

89	RevCrt	%l %s %s	Solicitud de revocación.	si	CrtNoRev, CrtRev, CrtRevNoExiste, CrtRevCad, CrtYaRev.
86	AltaCrtAut	%l %s %s	Solicitud de alta de certificado.	si	CrtAceptado, CrtRechazado.
85	RevCrtAut	%l %s %s	Solicitud de revocación.	si	CrtNoRev, CrtRev, CrtRevNoExiste, CrtRevCad, CrtYaRev.
82	IdAutMsg	%s	Aviso de número de AR.	no	
80	PideCrtNvoFmt	%s	Petición de certificado.	no	CrtNoExiste, AutNoConn, RegCrtNvoFmt.
79	LstRev		Solicitud de lista de revocación.	no	LstRevVacía, UnicoLstRev, IniLstTev, FinLstRev.
77	VerifCrtCorto	%s	Verificación de certificado.	no	CrtNoExiste, AutNoConn, RegCrtCorto.
76	IdFmaAleat ⁶	%s	Firma de número recibido.	si ⁷	LOGGED, Desconexión.

⁶En este mensaje en particular, lo que se manda es sólo una cadena, terminada en nulo, con la firma en base 64, del descifrado del mensaje `IdUsuarioAleat`. La longitud de la firma no se manda, pero en el encabezado del mensaje se debe colocar la cantidad de bytes enviados, esto es, la longitud de la firma más uno (por el carácter nulo).

⁷Se pone que sí va firmado, porque lo que se manda es una firma, pero no es igual al resto de los mensajes firmados. De hecho se puede tratar como un mensaje normal, sin firma.

En la siguiente tabla se muestran los mensajes enviados por la IES (ARC y AR de Banxico) a los clientes.

No.	Nombre	Formato	Descripción	Firma
183	IdUsuarioAleat	%l %s	Identificación del usuario.	si
184	CrtRevNoExiste	%l %l %s	Certificado a revocar no existe.	si
185	CrtRevCad	%l %l %s	Certificado a revocar caduco.	si
186	CrtYaRev	%l %l %s	Certificado revocado anteriormente.	si
187	RegCrtCorto	%l %d %l %l %l %s %s	Regreso de certificado en formato corto.	si
188	LstRevVacía		Aviso de vacuidad en lista de revocados.	no
189	UnicoLstRev	%l %ln(%s %l)	Un sólo listado de revocados.	si
190	FinLstRev	%l %ln(%s %l)	Aviso de fin de lista de revocados	si
191	SigLstRev	%l %ln(%s %l)	Aviso de continuación de lista de revocados.	si
192	IniLstRev		Aviso de inicio de lista de revocados.	si
193	CrtEnAlerta	%l %l %s	Aviso de certificado comprometido. <i>NOTA: Ver la descripción de este mensaje para más detalle</i>	si

194	CrtNoExiste	%l %l %s	Aviso de inexistencia de certificado.	si
195	RegCrtNvoFmt	%l %d %l %l %l %s	Envío del certificado en formato corto.	si
197	AutNoConn	%l %l %s	Aviso de autoridad fuera de línea.	si
204	CrtAceptado	%l %l %s	Respuesta de registro de certificado exitoso.	si
241	CrtRev	%l %l %s	Respuesta de revocación de certificado exitosa.	si
242	CrtNoRev	%l %l %s	Respuesta de revocación de certificado fallida.	si
243	CrtRechazado	%l %l %s	Respuesta de registro de certificado fallido.	si
253	LOGGED		Respuesta de aceptación de conexión.	no
203	OprNoPermit		Aviso de operación no permitida por el usuario.	no
50	TipoDesc		Aviso de tipo de petición desconocida.	no
255	LogoutAut	%l %d %l	Desconexión de AR o AC a solicitud de la ARC	si

La interpretación de cada uno de los mensajes se muestra a continuación:

- LOGOUT** Este mensaje lo utiliza el cliente para avisar que cerrará su conexión.
- ConnUsr** La información enviada es el tamaño de la firma y el número de certificado del usuario.
- ConnAut** La información enviada es el tamaño de la firma y el número de certificado de la Autoridad.
- RevBrdcst** Este mensaje se envía a todos los usuarios conectados con la IES al momento en que un certificado sea revocado. La información que contiene el cuerpo del mensaje es el tamaño de la firma, la fecha de revocación y el número de serie del certificado revocado.
- AltaCrt** La información que se envía es el tamaño de la firma, el challenge-password cifrado con la clave pública de la entidad a la que se le hace la petición y el certificado.
- RevCrt** La información que se envía es el tamaño de la firma, el challenge-password cifrado con la clave pública de la entidad a la que se le hace la petición y el número de certificado.
- AltaCrtAut** La información que se envía es el tamaño de la firma, el challenge-password cifrado con la clave pública de la ARC y el certificado.
- RevCrtAut** La información que se envía es el tamaño de la firma, el challenge-password cifrado con la clave pública de la ARC y el número de certificado.
- IdAutMsg** Se envía a la ARC el número de AR que se ha conectado.
- PideCrtNvoFmt** La información que se envía es el número del certificado a consultar.
- LstRev** El cliente solicita lista de revocación.
- VerifCrtCorto** La información que se envía es el número del certificado a consultar. *Este mensaje se eliminará en versiones posteriores del protocolo, sustituyéndolo por PideCrtNvoFmt.*
- IdFmaAleat** La información que se envía es únicamente la firma del valor aleatorio recibido dentro del protocolo de identificación. Básicamente este mensaje no tiene cuerpo, ya que únicamente viaja una firma.
- IdUsuarioAleat** La información que se envía es el tamaño de la firma y un valor aleatorio cifrado con la clave pública del usuario a conectarse. Esto es parte del protocolo de identificación.
- CrtRevNoExiste** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado.

- CrtRevCad** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado.
- CrtYaRev** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado.
- RegCrtCorto** La información que se envía es el tamaño de la firma, el estado del certificado (válido = 0, revocado = 1, alerta = 2 y caduco = 3), la fecha de caducidad del certificado, la fecha de registro ante la IES, la fecha en que se genera el mensaje, el número de certificado y la digestión del certificado. *Este mensaje se eliminará en versiones posteriores del protocolo, sustituyéndolo por RegCrtNvoFmt.*
- LstRevVacia** Se avisa que no ha habido revocaciones en el día, es decir, la lista de certificados revocados está vacía.
- UnicoLstRev** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y “n” números de certificados con sus correspondientes fechas de revocación.
- FinLstRev** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y “n” números de certificados con sus correspondientes fechas de revocación.
- SigLstRev** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y “n” números de certificados con sus correspondientes fechas de revocación.
- IniLstRev** Se avisa que se inicia el envío de la lista de revocación en más de un mensaje.
- CrtEnAlerta** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado. Se deberá revocar el certificado recibido y **notificar a la ARC** de dicha revocación mediante el mensaje **RevBrdcst**
- CrtNoExiste** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado.
- RegCrtNvoFmt** La información que se envía es el tamaño de la firma, el estado del certificado (válido = 0, revocado = 1, alerta = 2 y caduco = 3), la fecha de caducidad del certificado, la fecha de registro ante la IES, la fecha en que se genera el mensaje y el certificado.
- AutNoConn** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado que se pretendía verificar.
- CrtAceptado** La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y número de certificado aceptado.

CrtRev La información que se envía es el tamaño de la firma, la fecha en que se revocó el certificado y el número del certificado ya revocado.

CrtNoRev La información que se envía es el tamaño de la firma, la fecha en que se rechazó el certificado y el número del certificado.

CrtRechazado La información que se envía es el tamaño de la firma, la fecha en que se genera el mensaje y el número de certificado rechazado.

LOGGED Aviso al cliente que se ha aceptado la conexión.

QprNoPermit Aviso al cliente que esa operación no es válida o no está permitida.

TipoDesc Aviso al cliente que el tipo de petición hecha por éste es desconocida.

LogoutAut Mensaje enviado únicamente por la ARC para notificar a una AR o AC que debe desconectarse. La información que se envía es el tamaño de la firma, el código de desconexión (de momento igual a cero) y la estampa de tiempo en que se produce el mensaje.

5. Comentarios

Para comentarios, dudas y/o sugerencias sobre este protocolo, por favor envíe un correo electrónico a la cuenta *ies@banxico.org.mx*