FIRMAS DIGITALES SRL
líder del mercado criptográfico argentino
Leandro N. Alem 1080 2° "C" (C1001AAS) - Buenos Aires - ARGENTINA
Tel (+54-11) 4314-8972 / 4970-6665 / 4403-4230 - Fax (+54-11) 4314-8973
Web site: http://www.fd.com.ar E-mail: info@fd.com.ar

SISTEMA DE FIRMA ELECTRÓNICA Y SU SINCRONIZACION DE TIEMPO UTC/GMT

1. Sistema de sincronización

Nuestro sistema de firma electrónica se implementa en dos modalidades, *sincronización por eventos* o *sincronización temporal*. Para los miniCD (CD Card) se optó por la segunda alternativa, es decir para que el sistema funcione correctamente, tanto el cliente (el mini CD o soporte equivalente) como el servidor (la página web donde se autentica al cliente) deben trabajar con la misma hora.

Los miniCD clientes (v.4.x) están preparados para trabajar en dos formas:

- Por *default*, cuando logran sincronizarse vía Internet, trabajan con la fecha-hora UTC (Universal Time Clock) GMT (Greenwich Meridian Time) -3 (hora oficial argentina en temporada normal). En este caso el LED frontal de la calculadora se pone verde y en la parte superior aparece la dirección TCP/IP del Host (servidor de tiempo o reloj atómico público). Aquí se muestra una imagen del cliente correctamente sincronizado en GMT-3 gracias a una consulta al reloj atómico *time-b.nist.gov* (129.6.15.29) *NIST, Gaithersburg, Maryland* según se lee en la parte superior izquierda de la calculadora*:*

- Cuando por algún motivo no logran sincronizarse vía Internet, trabajan con la fecha-hora de la PC cliente. Esto se manifiesta por el LED en color rojo tal como se muestra aquí:

Leandro N. Alem 1080 2° "C" (C1001AAS) - Buenos Aires - ARGENTINA
Tel (+54-11) 4314-8972 / 4970-6665 / 4403-4230 - Fax (+54-11) 4314-8973
Web site: http://www.fd.com.ar E-mail: info@fd.com.ar

Obviamente, en condiciones normales el servidor debe prepararse para recibir *tokens* (valores de firma electrónica) en GMT-3, pero hay situaciones especiales que hay que tener en cuenta y que se detallan mas adelante. Justamente por trabajar (por *default*) en GMT-3 y no en hora local es que el sistema se independiza de la política de horarios de la PC cliente y lo hace universal (se puede usar desde cualquier país).

***Nota:* si se hace un doble-click sobre el LED, se intercambia el estado de sincronización (siempre que no esté bloqueado el acceso a los servidores vía Internet), es decir pasará de Sincronización Internet a Hora Local y viceversa.**

2. Detalle técnico del sistema de sincronización cliente

El sistema de sincronización que emplea el sitio cliente KRYPTO-CD (o sea la calculadora del miniCD) está basado, en una conexión *on-line* usando el protocolo **Network Time Protocol** [**NTP v4.X**] – Normas Internacionales Provisionales RFC 867 /RFC 1305, ver referencias: http://www.faqs.org/rfcs/rfc867.html y http://tf.nist.gov/service/its.htm , en el cual cada cliente se conecta vía *port* 13 (TCP) a un *Atomic Clock Time Server* de uso público. Obviamente la política de seguridad del sitio cliente debe tener habilitado ese puerto, por ejemplo si un firewall bloquea TCP 13 no habrá sincronización vía Internet. La lista de servidores a los cuales intenta conectarse KRYPTO-CD (CD Card) está detallada en http://tf.nist.gov/tf-cgi/servers.cgi. El acceso se intenta siguiendo una lista circular y en caso de haberse logrado la conexión y una sincronización exitosa, el cliente pone su LED en color verde e indica la IP del Host accedido. En caso opuesto, ese LED quedará en color rojo y se generará el token (o valor de firma electrónica) con el *system time* de la PC cliente.

3. Problemas de sincronización

Una falla de sincronización se manifiesta cuando un legítimo cliente o usuario no logra autenticarse. Los problemas de sincronización surgen por dos orígenes:

- El programa cliente no logra sincronizarse en Internet (LED en rojo) y además su hora local no coincide con la hora local del servidor. Se recomienda que ambos se sincronicen con la hora oficial argentina (Normalmente, salvo horarios especiales de verano o invierno, GMT-3)

- El servidor no está sincronizado temporalmente (hora oficial argentina) y/o el software del sitio servidor no está correctamente preparado (nos referimos al script ***.asp*** y específicamente al correcto empleo del parámetro ***tokenDLL.delta*****,** aconsejamos consultar la documentación de instalación del sistema lado servidor FD-KRYPTOCD-SERVER-V12 y el documento FD-AUT-090-V10-CAMBIO HORA OFICIAL ARGENTINA).

Leandro N. Alem 1080 2° "C" (C1001AAS) - Buenos Aires - ARGENTINA
Tel (+54-11) 4314-8972 / 4970-6665 / 4403-4230 - Fax (+54-11) 4314-8973
Web site: http://www.fd.com.ar E-mail: info@fd.com.ar

Debe comprenderse que cualquier problema que surja con la sincronización sólo podrá solucionarse (razonablemente) desde el sitio servidor. Por ese motivo hemos incluido el valor ***tokenDLL.delta*** para poder compensar los desfasajes que pudiesen surgir.

Para ilustrar, si la Argentina decide pasar su Hora Oficial de GMT-3 a GMT-2, bastará con corregir el valor del Token (firma electrónica) dentro del rango de tolerancia (por ejemplo si se permiten valores token del rango 3 minutos antes y 3 minutos después del minuto actual según el *system time* del Server):

Donde decía:	Debe decir:
TokenDll.Delta = 3	TokenDll.Delta = -57
TokenDll.Delta = 2	TokenDll.Delta = -58
TokenDll.Delta = 1	TokenDll.Delta = -59
TokenDll.Delta = 0	TokenDll.Delta = -60
TokenDll.Delta = -1	TokenDll.Delta = -61
TokenDll.Delta = -2	TokenDll.Delta = -62
TokenDll.Delta = -3	TokenDll.Delta = -63

En cambio un pasaje de GMT-3 a GMT-4 se corregiría así:

Donde decía:	Debe decir:
TokenDll.Delta = 3	TokenDll.Delta = 63
TokenDll.Delta = 2	TokenDll.Delta = 62
TokenDll.Delta = 1	TokenDll.Delta = 61
TokenDll.Delta = 0	TokenDll.Delta = 60
TokenDll.Delta = -1	TokenDll.Delta = 59
TokenDll.Delta = -2	TokenDll.Delta = 58
TokenDll.Delta = -3	TokenDll.Delta = 57

Puede haber casos mas complicados, por ejemplo que algunas provincias adopten GMT-3 y otras GMT-2 u otro huso horario. Esto se corrige permitiendo autenticarse con cualquier combinación de husos en el script **.asp**. Por ejemplo, una provincia se encuentra en GMT-3 y el resto del país en GMT-2. La solución mas simple es que esto sea transparente al usuario y se corrige de la siguiente forma en el script:

```
informedToken=nnnnnn    { el valor que acaba de informar el usuario, no sabemos si es GMT-3 o GMT-2}
Status="non-validated"  { comenzamos seteando un  flag en no-validado }

For Token.Delta = - 3 to +3  (habilitamos GMT-3 exacto)
    If (ingToken = informedToken)  then begin
                        Status="validated"
                        Break {exit loop}
        End if
 End For

For Token.Delta = - 57 to -63  (además ahora habilitamos GMT-3 a GMT-2)
    If (ingToken = informedToken)  then begin
                        Status="validated"
                        Break {exit loop}
        End if
 End For
```

Leandro N. Alem 1080 2° "C" (C1001AAS) - Buenos Aires - ARGENTINA
Tel (+54-11) 4314-8972 / 4970-6665 / 4403-4230 - Fax (+54-11) 4314-8973
Web site: http://www.fd.com.ar E-mail: info@fd.com.ar

```
For Token.Delta = xxx to yyy  (y por último habilitamos cualquier otro horario)
   If (ingToken = informedToken)  then begin
                        Status="validated"
                        Break {exit loop}
      End if
End For

Case of Status       { ahora decidimos}
   "validated"       : { le permitimos operar... }
   "non-validated" : { o lo rechazamos del sistema ... }
End Case
```

Exactamente este método se deberá aplicar si hubiesen problemas de conectividad a los relojes UTC/GMT de Internet (si se "cayeran" consistentemente los relojes atómicos o ciertos clientes no pudiesen trabajar *on-line*). Los clientes, aparte de no poder autenticarse acusarán LED en rojo. Supongamos que la Hora Oficial fuese GMT-2 (tanto los clientes como el servidor están sincronizados GMT-2) En este caso, además de considerar el desplazamiento Token.Delta según la tabla GMT-3 a GMT-2 arriba señalada, bastará con:

- Agregar al script **.asp** la habilitación delta cero que sincroniza cualquier hora local con la hora del servidor (si es que ambas están en igual huso):

```
For Token.Delta = - 3 to +3  (habilitamos delta cero)
   If (ingToken = informedToken)  then begin
                        Status="validated"
                        Break {exit loop}
      End if
End For
```

- Asegurarse que las PC clientes estén ajustadas a la misma Hora Oficial Argentina que esté usando el servidor. Si esto no fuese posible, por ejemplo en una provincia con otro huso horario, agregar la corrección que corresponda en el **.asp**.

4. Ajuste de la PC cliente o servidor a la Hora Oficial Argentina.

Bajo Win32/64 y con los SO actuales (2000, XP, Vista) hay que instruir al cliente para que configure su fecha-hora con sincronización periódica (diaria) y automática. Si el SO no permite ese ajuste, bastará con aconsejar la descarga e instalación de algún utilitario que lo permita (por ejemplo http://www.worldtimeserver.com/atomic-clock/)