CAPITULO 1. ATM

- **ATM**

El ATM Automated Teller Machines nació por los esfuerzos de estandarizar el Broadband ISDN a mediados de los 80.

Sus principios básicos son:

- Ser considerado como un medio de transferencia de datos basado en celdas de longitud fija. Cada celda consiste en bytes de información y un header que es usado principalmente para determinar el canal virtual y para realizar su apropiado ruteo. La integridad de secuenciamiento de la celda es preservada por el canal virtual.

- ATM está orientado a conexión. Los valores del header son asignados a cada sección de una conexión durante toda su duración. La señalización y la información de usuario son llevadas por canales virtuales separados.

- El campo de información de las celdas ATM es llevado en forma transparente a través de la red.

- Todos los servicios (voz, vídeo, datos) puede ser transportados vía ATM. Para acomodarse a los distintos servicios, provee una función de adaptación dentro de las celdas ATM que además proveen servicio de funciones específicas (recupero de celdas perdidas, etc.).

- Conmutación ATM

ATM es la culminación de todos los desarrollos en conmutación y transmisión en los últimos 20 años. Incluye el advenimiento de conmutación de paquetes y el cambio de cable coaxial a fibra óptica.

Cell relay es una evolución de la suma de frame relay más circuitos de conmutación de tasa variable.

Usa paquetes de longitud fija llamados celdas.

Los circuitos de conmutación de tasa variable tienen canales fijos. La conmutación por celdas permite la definición de canales virtuales con tasas de transmisión variables definidas dinámicamente. De frame relay, las celdas toman el control de errores y permiten más manejo de errores y con un mayor nivel lógico. La longitud fija de la celda reduce el overhead aún más permitiendo tasas de decenas a cientos de Mbps.

El sistema de celdas es igualmente eficiente con CBR ó VBR (Constant / Variable Bit Rate)

Se está ante una tecnología de conmutación CELL RELAY y una tecnología de transmisión SDH (Syncronous Digital Hierarchy) sobre fibra óptica.

Cell relay soporta VBR, CBR y variadas aplicaciones. SDH permite que grandes cantidades de datos sean transmitidos eficientemente en la red. La combinación de estas dos ideas juntas dan la base para el ATM.

La principal característica de ATM es la elasticidad para almacenar y luego conmutar la transmisión de datos ante congestionamiento de la línea de comunicación.

- UNI para ATM

Cada usuario se conectará a la red por medio de UNI (User Network Interfase) para ATM que se usan para conversión de tramas a celdas ATM y su re−ensamblamiento en el UNI de los puntos de partida y destino respectivamente.

- Esquemas de Red ATM
- ¿Qué clase de protocolo es ATM?

    - ATM fue diseñado para conmutar paquetes de poca longitud en Gb/segundo a través de grandes distancias.

    - En la red ATM la conexión punto a punto, el control de flujo y el ruteo son hechos al nivel de la celda ATM.

    - Es un protocolo diseñado para conmutar paquetes de 53 bytes de longitud fija.

    - Lo que puede resultar más relevante es cómo el ATM interactúa con redes TCP/IP e IP en general y con aplicaciones en particular. Un modelo conveniente para interfase ATM es considerarlo como otro port de comunicaciones del sistema. Esto sería que desde el punto de vista de software del sistema puede ser considerado como cualquier otro puerto para comunicación de datos. Por ejemplo: Para redes IP conectadas a backbones ATM el modelo no sería diferente que para un circuito virtual de conexiones en un link STM excepto que los paquetes IP sobre una red ATM serán fragmentados en celdas en el UNI y re−ensamblados en un paquete IP en el UNI del punto de destino.

    - Podría verse así:

Data

TCP/IP

IP

ATM Adaption Layer

ATM Datalink Layer

Physical Layer

    - En un port ATM el datagrama IP es fragmentado en celdas para lo cual se especifica un AAL (ATM Adaption Layer). La fragmentación y el re−ensamblado son hechos en el hardware del lado que envía y en el que recibe.

    - Un UCI adquirido en el momento de establecer la conexión se ubica en el header de cada celda y las celdas son transmitidas.

    - En el receptor las celdas son re−ensambladas en el hardware usando el AAL y el paquete original IP es reformulado y manejado hacia su destino por el UNI.

    - El AAL no es un header separado, está contenido en la sección de payload de la celda ATM.

    - Para la interfase directa a una celda ATM desde una aplicación nuevas interfases tienen que ser diseñadas en el software que pueden proveer a la aplicación con mejores y más rápidos mecanismos para establecer la conexión, transferir los datos, mantenerlos vivos, desecharlos e incluso proveer un

nivel de control de flujo.

- En este caso el software de procesamiento sería:

Application Streaming Data

OS interfase to Application

ATM virtual circuit managment

Driver to interfase to ATM

ATM

- Donde el circuito virtual de administración representa al software que interpreta las especificaciones del header ATM, establece y discontinúa las conexiones y responde a todas las señales standard del protocolo que es empleado por ATM en la UNI para la administración de la conexión.

- El layer físico.

Las especificaciones del layer físico no son parte explícita de la definición de ATM.

El SDH (Syncronous Digital Hierarchy) especifica cómo el payload es fragmentado y transportado sincrónicamente por la fibra óptica sin requerir que todos los links y nodos tengan los relojes sincronizados para la transmisión y el recupero de los datos.

- Flow control de ATM

La capacidad en Gb/segundo de una red ATM genera un set especial de requerimientos para el control de flujo. Si el control se realiza por feed back para el momento en que el mensaje de control sea recibido por la fuente ésta podría haber transmitido x Mbytes de datos aumentando la congestión y para cuando reaccione podría haber desaparecido la condición de congestión.

Las condiciones de congestión en redes ATM deben ser extremadamente dinámicas requiriendo mecanismos de hardware rápidos para reactivar la red así como necesitan que la red actúe en el descongestionamiento.

Es recomendable un conjunto de reglas de control de flujo con una excelente alocación de recursos y un buen dimensionamiento de las redes para todos juntos tratar de evitar el congestionamiento, para detectarlo y tratarlo en cuanto se produzca en forma temprana con un exhaustivo monitoreo de las colas dentro de los switches ATM y reaccionando gradualmente a medida que las colas alcanzan determinados topes.

El estado de la red puede ser comunicado al UNI por la red rápidamente generando una celda de flow control siempre que una celda va a ser descartada en algún nodo debido a la congestión.

El UNI puede entonces controlar la conexión cambiando su tasa de injection ó notificar al usuario enganchado para la administración de los datos dependiendo del nivel de severidad de las condiciones de congestión.

La mayor tarea para el flow control es tratar de afectar sólo a las conexiones que son responsables de la congestión y no a las demás y así mismo permitir a una conexión utilizar tanto ancho de banda como necesite si no hay congestión.

- Modo de transferencia asincrónico.

ATM es un protocolo que transmite datos como paquetes de longitud fija. Es la culminación de todos los desarrollos de conmutación y transmisión de datos de los últimos 20 años.

Fue usado para hacer una realidad la B−ISDN que funciona como red de comunicación que puede proveer servicios integrados como transmisión de datos a alta velocidad, video, video conferencias, CATV además de teléfono y telex.

Para estos servicios era necesaria una interfase entre los layers de más alta jerarquía y el layer ATM.

El AAL (ATM Adaption Layer) provee este servicio. Su principal propósito es resolver cualquier disparidad entre un servicio requerido por usuario y los servicios disponibles en ATM.

Esto está entre el layer ATM y los layers de más alta jerarquía del protocolo B−ISDN

La celda ATM es la unidad básica de transferencia de información en el protocolo ATM. Comprende 53 bytes, cinco de ellos constituyen el campo header y los 48 restantes son de datos.

Las celdas ATM son transportadas por canales virtuales (VP) e indirectamente por paths o caminos virtuales (VP). Un VC es una vía unidireccional, un VP es un conjunto de VC.

Las celdas viajan a través de los VC necesitando para ello un medio físico (por ej. Fibra óptica).

La función principal del layer físico es colectar y organizar las celdas ATM enviadas desde el layer ATM, transportarlas al medio físico y hacer la reversa del proceso.

Una red ATM necesita cierta capacidad de control de tráfico para aplicaciones como video conferencias que necesitan una cierta cantidad garantizada de ancho de banda disponible, además de usar la red de la forma más eficiente posible y manejar errores potenciales de la red en cualquier momento.

- Los AAL (ATM Adaption Layer)

Están entre el layer ATM y los layers de más alto nivel que usan servicios ATM. Y su principal función es resolver cualquier disparidad entre un servicio requerido por el usuario y los servicios disponibles en el layer ATM.

El AAL mapea información de usuario en celdas ATM. Puede transportar información de timing tal que el destinatario puede regenerar señales que dependen del tiempo.

La información transportada por el AAL está dividida en distintas clases de acuerdo a las siguientes propiedades:

- La información que está siendo transportada es tiempo dependiente ó independiente.
- Tasa variable ó constante de bits/segundo.
- Modo de transferencia de información con ó sin conexión

Estas propiedades definen 8 posibles clases, 4 de las cuales están definidas como **CLASES DE SERVICIO.**

- La celda ATM

La siguiente es la estructura de una celda ATM NNI (Network Node Interfase)

- UNI

La siguiente es la estructura del UNI (User Network Interfase)

El campo header está dividido en campos. El tamaño de los bits asociados difiere poco entre NNI y el UNI y son

- *Generic Flow Control*

Aún cuando su principal función es el control del acceso físico es a menudo usado para control de tráfico.

Funcionalmente requiere el poder de controlar cualquier estructura UNI, sea anillo, estrella, bus o cualquier combinación.

- *Virtual Path Identifier / Virtual Channel Identifier*

Es la combinación de dos números tal que las celdas que pertenecen a la misma conexión puedan ser distinguidas.

Un único par VPI/VCI es asignado para indicar qué tipo de celda sigue.

- *Payload Type / Cell Loss Priority / Header Error Control*

Cuando la información de usuario está presente ó la celda ATM ha sufrido congestión de tráfico el campo PT lleva esta información.

El bit CLP se usa para decirle al sistema si la correspondiente celda debe ser descartada durante la congestión de la red. Las celdas ATM con CLP = 0 tienen prioridad ante pérdidas sobre las celdas con CLP = 1, en otras palabras, durante una congestión de recursos las celdas con CLP = 1 son descartadas antes que cualquiera con CLP = 0.

El HEC es un byte en la cabecera de la celda y es usado para corregir errores de la celda y delimitar la cabecera de la misma.

- Physical Layer

El PL tiene distintas formas pero su propósito principal es juntar y organizar las celdas ATM enviadas desde el layer ATM, transportarlas al medio físico y también efectuar la reversa del proceso.

Debe proveer otras funciones como por ejemplo chequeo de errores y control.

Se divide en dos partes:

- Convergencia de transmisión
- Medio físico

Dentro de la convergencia de transmisión encontramos el HEC (Header Error Control) que es generado para los 4 primeros bytes del header de la celda ATM e insertado en el quinto byte. Aplica el proceso inverso en la dirección contraria para detectar errores.

El medio físico depende del medio de transmisión, si por ejemplo se usa fibra óptica la función estará

relacionada con este medio en particular

- *HEC*

Luego del proceso del HEC la celda ATM es identificada como válida ó inválida.

Las celdas válidas pueden contener errores por falla en el estadío de corrección de errores. Estas celdas inválidas son la principal causa en la degradación de la performance del ATM.

El código usado por el HEC es cíclico con generación polinomial. Los 4 primeros bytes escritos como polinomio son sujetos a otra operaciones y el resto de la última división es grabado en el HEC que luego es confirmado por el receptor usando el algoritmo inverso.

- Relación entre ATM y B−ISDN

ATM hizo de B−ISDN una realidad. Pero no nos da una idea apropiada de cómo la relación se produjo. El ISDN evolucionó durante los 80 hacia un canal básico que podía operar a 64kbps. Y la combinación de éste con otros formó la base de la comunicaciones en la red.

Sin embargo, al mismo tiempo, la demanda de comunicación de alta velocidad y comunicación de video se incrementó.

Para video, redes de CATV, video conferencias, etc, llevaron a la necesidad de servicios de mayor velocidad y servicios de broadband además de los clásicos de teléfono y telex.

Esta diversidad de servicios significa velocidades de transmisión de 155 Mbps, 622 Mbps y 2.4 Gbps y conmutación a estas mismas velocidades.

- Control de tráfico ATM

Una red ATM necesita capacidades para trabajar con distintas clases de servicio con errores potenciales en la red en cualquier momento.

La red debería tener las siguientes capacidades de control de tráfico:

- *Administración de recursos de la red*

Usando la técnica de los VP agrupando canales virtuales otros tipos de control pueden resultar más simples, por ejemplo el control de la admisión de conexión y parámetros de control de uso y de control de la red. Sólo el tráfico colectivo de un VP tiene que ser manejado.

Los mensajes para la operación de control de tráfico pueden ser mejor distribuídos.

Las formas de control pueden ser simplificadas

- *Control de admisión de conexión*

Grupo de acciones tomadas por la red durante la fase de llamada para seteo para establecer si un VP ó VC puede ser aceptado por la red. Esto puede suceder sólo si hay suficiente cantidad de recursos disponibles para establecer la conexión end−to−end con suficiente calidad de servicio. La calidad de servicio pre−concertada no debe ser afectada por la nueva conexión.

- *Parámetros para control de uso y control de la red*

Ambos hacen el mismo trabajo en distintas interfases, la función de UPC es realizada en la interfase de usuario, la NPC es la interfase de nodo de la red.

Ambos protegen los recursos de la red de daños, intencionales ó no, que puedan afectar la calidad de servicio

  - Chequean la validez de VPI/VCI
  - Monitorean el volumen de tráfico que entra a la red desde cualquier conexión
  - VP/VC para controlar que los parámetros acordados no sean violados
  - Monitorean el volumen total del tráfico aceptado en el link de acceso

- *Control de prioridad*

Las celdas ATM tienen un bit especial en el header que diferencia dos clases de prioridades. Una sóla conexión ATM puede tener ambas clases de prioridad cuando la información a ser transmitida es clasificada en partes más y menos importantes.

- *Traffic shapping*

Altera las características de tráfico de una sucesión de celdas en un VPC ó VCC para reducir la tasa de transmisión evitando colapsos.

De las celdas, limita el largo de BURST ó reduce la variación de demora espaciando las celdas en el tiempo. Esto por supuesto dentro de los limites de la integridad de secuencia de una conexión ATM. Es una opción para operadores y usuarios de la red ATM

- *Control de congestión*

Es un medio de minimizar los efectos de la congestión y prevenir sus consecuencias. Puede emplear admisión de conexión ó parámetros de control de uso y parámetros de control de red para evitar situaciones de congestionamiento.

En estos casos advierte que la red no puede garantizar los valores de calidad de servicio esperados. Puede producirse por más tráfico del estadísticamente esperado o por fallas de la red.

- *Virtual Channel / Virtual Path*

ATM provee dos tipos de conexiones de transporte, VP y VC.

VC es una conexión uni direccional hecha por la concatenación de una secuencia de elementos de conexión.

Un VP es un grupo de estos canales.

Cada canal y path tiene un identificador asociado con él. Todos los canales en un path tienen identificadores distintivos pero pueden tener la misma identificación que otro canal asociado con otro path.

Un canal individual puede ser identificado unívocamente por su número de canal y path.

El número de canal virtual y path de una conexión pueden diferir del emisor al receptor si la conexión es switcheada en algún punto de la red.

Los VC que permanecen en un solo VP a través de las conexiones tendrán idénticos identificadores de canal virtual en ambos extremos (end point). La secuencia de celdas es mantenida por la conexión del VC.

- Servicio ATM − Clases de Servicios

- **Transmisión segura de Documentación− Firma Digital**
- Esquema Digital.
- Descripción

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura , que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dio lugar al concepto. Pero sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas (jurídicas o reales).

Se intenta hacer coincidir el modelo de firma digital con los requerimientos y virtudes que debe tener una firma y así darle validez a esta mecánica. El fin es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado.

El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará señales identificables.

Pero estas mismas cualidades traen aparejados inconvenientes que el uso de sistemas de computación podría evitar. Ciertamente los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al rescatarlos), y el compartir los documentos también resulta inconveniente.

- Ventajas Ofrecidas por la Firma Digital

El uso de la firma digital satisface los siguientes aspectos de seguridad:

- Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

- Autenticidad del origen del mensaje*:* este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como

emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

- No repudio del origen*:* el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

- Aspectos técnicos

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje.

Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original.

En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública−privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.

A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

- Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad).

- Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad).

- El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio).

El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro.

Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.

Si bien no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de

cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye.

Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad y no repudio del origen), pero no se satisface el concepto de confidencialidad de la información (secreto).

- Necesidad de legislar sobre la firma digital

En las reformas realizadas al Código Civil argentino no se ha tratado en forma expresa el problema de las nuevas tecnologías y en especial la utilización de documentos digitales. En los últimos años, principalmente en Europa y en Estados Unidos, las leyes han sido modificadas para adaptar el sistema de firmas digitales.

Ciertas normas especiales como la ley de sociedades o de procedimiento tributario autorizaron el registro de datos en medios informáticos o la emisión de certificados de deuda con firma mecanizada, pero en principio y como regla de nuestro derecho, la forma de los actos jurídicos, cuando se trata de documentos escritos, no puede desligarse del papel y de la firma tradicional.

Los obstáculos para el reconocimiento del documento electrónico son:

- ***Escritura***: la escritura puede ser impresa, mecanografiada o manuscrita, salvo la firma que, por su índole, tendrá que ser de esta última calidad.

- ***Firma:*** el art. 1012 del Código Civil dice que la firma es condición esencial para la existencia de todo acto bajo forma privada. La firma es el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad.

De esto se desprende que no puede sostenerse que un conjunto de claves pública−privada por la cual se encripta un documento digital constituye la firma que requiere nuestra legislación civil.

Aunque siempre queda la posibilidad que las partes, mediante un convenio de derecho privado, establezcan las características de un sistema informático por el cual se vincularán electrónicamente, la falta de generalidad de esta norma (ese convenio solo rige para el caso particular) y la inseguridad jurídica que sugiere el uso de medios no contemplados por la ley ha obstaculizado el desarrollo de esta nueva tecnología de firma digital.

Esos límites que impone la ley se solucionarían con una reforma integral de nuestro sistema de derecho privado que incorpore el mecanismo de firma digital equiparándolo a la firma tradicional.

- Situación en otros Países
- Firma Digital en Alemania

En Alemania la firma digital es un sello integrado en datos digitales, creado con una clave privada que permite identificar al propietario de la firma y comprobar que los datos no han sido alterados.

- Firma Digital en Naciones Unidas

En las Naciones Unidas una firma digital o numérica es un valor numérico que se consigna en un mensaje de datos y que, gracias al empleo de un procedimiento matemático conocido y vinculado a la clave criptográfica privada del originante, logra identificar que dicho valor se ha obtenido exclusivamente con la clave privada de iniciador del mensaje.

Los procedimiento matemáticos utilizados para generar firmas numéricas autorizadas, se basan en el cifrado de la clave pública. Estos procedimientos aplicados a un mensaje de datos, operan una transformación del mensaje a fin que el receptor del mensaje y poseedor de la clave pública del originante pueda establecer:

- Si la transformación se efectuó utilizando la clave criptográfica privada que corresponde a la clave pública que él tiene como válida.
- Si el mensaje inicial ha sido modificado.

- Situación Actual en la Argentina

En la Argentina la firma digital es el resultado de una transformación de un documento digital empleando un criptosistema asimétrico y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda establecer con exactitud.

- Si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del originante, lo que impide su repudio.
- Si el documento digital ha sido modificado desde que se efectuó su transformación, lo que garantiza su integridad.

- Uso de documentos digitales en la Administración Pública Nacional

El primer antecedente que autorizó el uso de documentos digitales dentro de la Administración Pública Nacional es el art. 30 de la ley 24.624 (Boletín Oficial 29/12/95) reglamentado posteriormente por la Decisión Administrativa No. 43/96 (Boletín Oficial 7/5/96).

Mediante esta normativa se autorizó al Archivo General de la Administración a transformar sus documentos originales a soporte electrónico u óptico indeleble, mediante el procedimiento que se establece en la respectiva reglamentación.

Con esta reforma se abrió la posibilidad de digitalizar la documentación administrativa del Estado, pero sólo con fines de archivo. No existía hasta la fecha una normativa de carácter general que regulara el procedimiento administrativo informatizado, permitiendo prescindir del expediente tradicional (en papel) y reemplazarlo por mensajes electrónicos. Fue así como se formó un comité en el ámbito de la Secretaría de la Función Pública que se dedicó al estudio de la implementación de la firma digital dentro de la administración pública.

Publicada en el Boletín Oficial del 24 de marzo de 1997, la resolución No. 45/97 de la Secretaría de la Función Pública constituye la primera norma nacional que introdujo en nuestro derecho un marco normativo para la incorporación de la tecnología de firma digital en los procesos de información del sector público. Esta norma tiene por finalidad contemplar estándares tecnológicos de mínima que aseguren la determinación de la autoría de la firma digital y la inalterabilidad del contenido del documento digital suscrito.

Establece una serie de requisitos que deben ser entendidos como pautas o guías para el caso que se decida establecer una regulación que contemple esta tecnología. Ellas son:

- *Documentos digitales oponibles a terceros*: esto implica que el documento digital requiere que la firma digital permita la identificación del emisor o autor y la integridad de su contenido.

- *Equiparación de la firma digital a la firma ológrafa:* este punto constituye la esencia de la normativa al permitir que quienes opten por utilizar documentos digitales suscritos digitalmente obtengan garantías legales similares a las que brinda la firma ológrafa sobre el soporte de papel. La firma ológrafa permite, simultáneamente, identificar a su autor así como imputarle la autoría del texto que la

precede.

- *Uso de la criptografía asimétrica como medio para instrumentar la firma digital:* la criptografía asimétrica o de clave pública constituye el único método actualmente capaz de implementar la firma digital, pues cumple con las características esenciales de la firma ológrafa, es decir, que permite simultáneamente identificar en forma inequívoca al autor y verificar sin lugar a dudas que el mensaje no ha sido alterado desde el momento de su firma. Este mecanismo es el único que no requiere la divulgación de la clave privada (secreta) utilizada por el firmante para suscribir el documento.

- *Autoridades certificantes de claves públicas y privadas:* esta autoridad certifica la correspondencia entre una clave pública y la persona física o jurídica titular de la misma. En forma similar a lo que ocurre con las entidades verificadoras de dominios en Internet, sería posible acudir a las autoridades certificantes para saber de manera inequívoca si una clave pública corresponde a quien debería.

El Anexo de la Resolución 45/97 concluye que la firma digital permitirá:

- La digitalización de cualquier circuito de la información, incluyendo documentos legales que normalmente requieren firmas y sellos convencionales.

- La generalización de la utilización de firma digital a través de la adopción de pautas uniformes que permitan verificar la autenticidad e integridad de los documentos digitales que requieran firma para su validez.

- Un menor riesgo de fraude en los documentos digitales suscritos digitalmente.

El martes 21 de abril de 1998 se publicó en el Boletín Oficial el decreto 427/98 que fija el Régimen al que se ajustará el empleo de la firma digital en la instrumentación de los actos internos, que no produzcan efectos jurídicos individuales en forma directa, que tendrá los mismos efectos de la firma ológrafa. Autoridad de aplicación.

Basándose en la normativa que ya había sido dictada y aplicada anteriormente, los objetivos de este decreto son:

- Eliminar el uso del papel y automatizar los circuitos administrativos mediante la introducción de tecnología de última generación incluyendo el uso de la firma digital que posee la misma o superior garantía de confianza que la firma ológrafa.

- Designar a la Secretaría de la Función Pública como Autoridad de aplicación para, entre otras cosas, dictar los manuales de procedimiento de las Autoridades Certificantes Licenciadas y de los Organismos Auditante y Licenciante, la fijación de los estándares tecnológicos aplicables a las claves. Debiendo cumplir esta tarea en un plazo de seis meses a partir de la fecha de publicación.

- Se adjunta a los considerandos del decreto el Anexo I con las condiciones definidas en la Infraestructura de la Firma Digital para el Sector Público Nacional.

En el Anexo I mencionado se definen los conceptos de las distintas partes intervinientes, sus funciones y obligaciones:

- ***Organismo Licenciante***: es el que otorga las licencias habilitantes para acreditar a las Autoridades Certificantes y emite los correspondientes Certificados de Clave Pública, debiendo abstenerse de acceder, absolutamente, a la clave privada de cualquier suscriptor de los certificados que emitan.

- ***Organismo Auditante:*** es el que audita periódicamente al Organismo Licenciante y a las Autoridades Certificantes Licenciadas, evaluando la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos.

- ***Autoridad Certificante Licenciada:*** tiene a su cargo la emisión de los Certificados de Clave Pública, debe abstenerse de acceder a las claves privadas de los suscriptores, y utilizar sistemas generadores de claves técnicamente confiables.

- ***Suscriptor de Certificado de Clave Pública:*** debe proveer a la Autoridad Certificante Licenciada todos los datos requeridos por esta, mantener el control de su clave privada e impedir su divulgación.

- ***Certificados de Clave Pública:*** enumera los datos que deben contener los Certificados de Clave Pública.

Actualmente se está trabajando en un proyecto de ley para normar este tema a nivel nacional en los ámbitos público y privado.

- Uso de documentos digitales en el ámbito privado

Como se desprende de lo expuesto hasta este punto, en el ámbito privado no existen leyes que regulen la utilización de la firma digital.

Pero las ventajas que brinda este sistema hace que cada vez haya más entidades que se adhieren al mismo, instrumentando los procedimientos necesarios para la operatoria en un marco legal de Derecho Privado (acuerdo entre las partes).

Se utilizan lo que se denominan VAN (Valued Added Networks) o redes de valor agregado que, sin utilizar Internet, permiten establecer un vínculo seguro con la otra u otras partes.

Por otro lado, los esquemas de encripción, manejo de claves, etc. se hacen siguiendo estándares internacionalmente aceptados que brindan no solo los aspectos de seguridad ya mencionados al comienzo, sino también ***confidencialidad*** mediante el uso de encripción del texto completo del mensaje (EDI − Electronic Data Interchange)

- *¿Cuál es el principal inconveniente?*

Hasta ahora se trata de la ausencia de un Ente o Autoridad Certificante. Cuando se trata de entidades de primer nivel se estila que cada una actúe como Autoridad Certificante pero lo ideal para poder extender la utilización de este método es su designación a través de una ley. La propuesta que se estudia con mayores posibilidades de ser la que finalmente se acepte, es que sea el Colegio de Escribanos.

- *EDI: Electronic Data Interchange*

EDI es el intercambio Electrónico de Documentos Comerciales en formato estandarizado entre las aplicaciones informáticas de empresas relacionadas comercialmente. Este formato responde a un estándar internacional (EDIFACT/EANCOM) desarrollado por Naciones Unidas y actualmente utilizado en todo el mundo.

A nivel internacional, EDI es el sistema de intercambio de documentos electrónicos estandarizados mas difundido. A lo largo de los últimos años ha crecido exponencialmente en los países desarrollados tales como E.E.U.U., Japón y países de Europa. A nivel Regional, específicamente en América Latina, recién esta dando sus primeros pasos.

A continuación se detalla una lista de algunos de los Documentos Estándar disponibles para establecer la comunicación entre entidades:

PARTIN: Este documento proporcionará la información de las partes.

PRICAT: Catálogos de artículos.

ORDERS: Ordenes de compra.

ORDRSP: Respuesta a la orden de compra.

DESADV: Aviso de despacho.

RECADV: Aviso de recibo

INVOIC: Factura

PAYMUL: Orden de pago

DEBMUL: Aviso de débito

CREMUL: Aviso de crédito

REMADV: Aviso de remesa

Algunos de los beneficios que aporta el comunicarse a través de este estándar son:

- Información rápida y precisa en el lugar indicado.
- Permite un mejor planeamiento de la recepción y el despacho de mensajes.
- Seguridad en el procesamiento de transacciones, se eliminan los errores por el reingreso de información disminuyendo así los problemas generados en la conciliación de facturas y la subsiguiente confección de débitos y créditos.
- Reducción de costos administrativos.
- Disminuye notablemente la cantidad de documentos impresos.
- Fortalece la relación comercial de los socios del negocio.
- Comunicación permanente las 24 horas los 365 días del año.
- Mejora notablemente la relación comercial de los socios del negocio.

- *Los componentes de un Sistema EDI*

Los tres componentes o estructuras de un sistema EDI son los mensajes estándares, los programas EDI y las (tele) comunicaciones. Para que las empresas estén en condiciones de operar utilizando un Sistema EDI deberán estar en condiciones de manejar los componentes que a continuación se detallan.

- *Mensajes Estándares*

EDI y los mensajes estándares han llegado a ser inter−dependientes a medida que el EDI ha progresado desde sistemas propietarios, sistemas cerrados en un entorno único, a sistemas abiertos.

Las distintas aplicaciones que se comunican entre sí necesitan una lengua común con el fin de comprenderse unas con otras.

Este lenguaje común se encuentra en los mensajes estándares EDI y más concretamente en UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Transport), los mensajes estándar internacionales EDI y la guías de implementación de UN/ EDIFACT tales como EANCOM.

- *Programas que Soportan EDI*

La función básica de los programas que soportan EDI, generalmente conocidos como los convertidores EDI, consiste en la traducción de los mensajes entrantes desde un mensaje estándar tal como EDIFACT/ EANCOM a un formato interno de archivo de una compañía, y el proceso inverso para mensajes que salen de la misma.

Sin embargo, además de la función de convertidor, los paquetes de EDI contienen también otras funciones adicionales, las cuales generalmente incluyen conversión de múltiples mensajes estándares y versiones de mensaje, mantenimiento de perfiles de los socios de negocios, interfaces de aplicación, módulos de comunicaciones para intercambiar información directamente o por medio de una o más redes de valor agregado, información de administración de mensajes salientes y entrantes incluyendo referencias para auditoría; manuales sobre menús referentes a los módulos de recibo de información y seguridad o control de acceso a través de contraseñas.

- *Comunicaciones y Redes de EDI*

Una vez que los datos de una aplicación se han convertido desde un archivo con formato interno al formato de mensaje estándar por medio del software de EDI, los datos deben ser comunicados o físicamente transferidos al receptor del mensaje.

Aunque es posible transferir los datos por medios magnéticos tales como cintas o disquetes, las telecomunicaciones son parte esencial del concepto EDI.

Las comunicaciones de datos requieren algunas normas de disciplina para lograr una transferencia ordenada de información; esto se realiza mediante los protocolos de comunicación. Adicionalmente, habrá varias opciones de telecomunicaciones/redes que tendrán la función de ofrecer medios para la comunicación de datos. Algunas de estas opciones son la comunicación privada punto a punto, utilizando líneas arrendadas, el uso de la red telefónica pública de datos empaquetados o red de servicios de valor agregado ofrecidas por compañías especializadas.

- *Costos del Proyecto EDI*

Encarar un proyecto de este estilo en una empresa no es una tarea sencilla por cuanto se deben considerar los costos que implica la adopción de este nuevo estilo de trabajo, no solo por los cambios tecnológicos sino por los cambios culturales que implica.

Entre los aspectos más destacados en cuanto costos resaltamos:

- Estratégicos, o aquellos costos que insume el tiempo invertido en el planeamiento de todo lo que tenga que ver con el sistema EDI. Este costo implica el tiempo que se tomará el área Gerencial de la entidad en tomar la decisión de implementar EDI, analizando Políticas de Implementación, Desarrollo, el estudio Económico y el Impacto que la nueva tecnología tendrá sobre las operaciones que actualmente se realizan.

- Desarrollo, adquisición de programas EDI, desarrollo y programación de las interfaces de aplicación, mejoramiento del software de aplicación interno para aprovechar todas las ventajas de un EDI integral y las pruebas necesarias para la óptima implementación de la nueva Tecnología.

- Educación, este aspecto incluye tanto el entrenamiento del personal interno para redefinir y asumir nuevas responsabilidades en un ambiente de EDI, como así también la educación de los socios de negocios.

- Implementación, incluye el costo del personal del área de Sistemas de Información que asegura la compatibilidad de las aplicaciones internas con los sistemas de los nuevos socios de negocios.

- Intercambios, son los costos asociados con el envío y recibo de mensajes EDI a través de redes privadas o redes de valor agregado. Este costo incluye tanto el Gasto en comunicaciones, como el mantenimiento de todos los elementos que permitan el óptimo funcionamiento de los programas EDI, ya sea Líneas Telefónicas, Cuentas de Usuario en la VAN, Servicio Técnico mensual de los Equipos, etc.

- *Beneficios del Proyecto EDI*

Los beneficios de la implementación de EDI se presentan al iniciar el proyecto, y los beneficios son más cualitativos e intangibles que cuantitativos. Los podemos sintetizar en los siguientes puntos:

- **Beneficios Administrativos y de Procesamiento**

Estos son probablemente los beneficios más tangibles obtenidos al implementar un sistema EDI. Los estimativos deben realizarse en el número de documento/ítems por línea procesados por año para cada documento en particular. Los costos relativos al procesamiento de tal documento deben incluir papelería preimpresa, sobres, estampillas, telex, teléfono, fax y costos de fotocopias.

Los estimativos deben ser hechos contemplando el tiempo que se gasta en consecución y ordenamiento de los datos, entrada de los mismos, mecanografía, fotocopias, archivo, correo y fax y lo más importante, en el control y corrección de errores de cada ítem por línea. El intercambio directo de datos entre una aplicación y otra eliminará los frecuentes y costosos errores que se producen inevitablemente cuando los datos son manejados e intercambiados manualmente.

- **Beneficios por la reducción del Ciclo de los Negocios**

Un sistema EDI exitoso reducirá substancialmente el tiempo de realización de una transacción, sea del tipo que fuere.

EDI no solamente conducirá a un ciclo de negocios mas rápido sino además, a una mejor calidad de la información compartida entre los socios de negocios.

- **Beneficios Estratégicos**

A pesar de que EDI tiene algunos costos y beneficios claros, es antes que todo una forma de hacer negocios, siendo los beneficios estratégicos los más importantes. Estos incluyen aspectos tales como mayor satisfacción del cliente, las mejores relaciones entre empresas y fortalecimiento de las relaciones de negocios. Otros beneficios estratégicos pueden incluir incrementos sostenidos en la participación en el mercado y ventajas competitivas.

Los beneficios estratégicos son difíciles de cuantificar pero presentan una respuesta a las necesidades del mercado. Aunque puede ser fácil demostrar que EDI conducirá a un incremento en la participación del mercado y cuantificar el valor de este incremento, será difícil predecir que tanto se incrementará esta participación gracias a un sistema EDI.

- *Seguridad de la Información Transmitida*

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos.

Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encripción de Datos. A continuación se realiza un breve comentario sobre métodos de encripción:

Para poder Encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:

Los algoritmos HASH, los simétricos y los asimétricos.

- **Algoritmo HASH:**

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

- **Algoritmos Simétricos:**

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactuan varios interlocutores.

- **Algoritmos Asimétricos (RSA):**

Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.

El usuario, ingresando su PIN genera la clave Publica y Privada necesarias. La clave Publica podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada.

Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica porque el utilizó su Clave Privada.

A continuación se muestra un listado con los proveedores con quienes actualmente se puede establecer comunicación mediante la utilización de EDI, que integran la VAN del SEA:

- **PROXTER.**
- **MOLINOS RIO DE LA PLATA**
- **MASTELLONE HNOS.**
- **SANCOR S.A.**
- **LEVER S.A.**
- **QUILMES.**
- **BUDWEISER.**
- **COCA COLA.**
- **PEPSICO.**

Estas son las Empresas que proveen del 75% de los productos que comercializa La Empresa. Obviamente existen muchas otras no enumeradas, que podrían incorporarse a la VAN, pero las mencionadas son las que

actualmente pueden implementar, y de hecho ya lo han hecho con otras Cadenas de Supermercados, y están en mejores condiciones técnicas de realizarlo.

En el momento de tomar la decisión, será muy importante seleccionar adecuadamente a los proveedores con quienes se iniciará la Implantación.

Lic. en Informática− UCS ATM y Firma Digital

Página Nº 32