Aurrera !

Boletín Divulgativo de Nuevas Tecnologías en Informática y Telecomunicaciones

Publicado por el Gabinete Tecnológico de la DIT

Nº 2

Diciembre de 2000

Enviad vuestras sugerencias a: **aurrera@ej-gv.es**

ÍNDICE

ESKERRIK ASKO!

Ya vamos por el segundo número del **Boletín Divulgativo AURRERA!,** desde el cual nos gustaría agradecer a todos los lectores la buena acogida y aceptación que tuvo nuestro primer número. Igualmente, aprovechamos la ocasión para agradecer al **Departamento de Industria** su colaboración en el apartado **"ALBOAN"** de nuestro primer ejemplar.

Por si no os acordáis , el apartado **"ALBOAN",** esta a vuestra entera disposición para que podáis dar a conocer al resto de los Departamentos del Gobierno Vasco vuestros proyectos, ideas, etc. Así que animamos al resto de departamentos a que realicen sus aportaciones y agradecemos su colaboración a todos los que nos han ayudado en este segundo ejemplar.

Por otro lado, indicar que en este número se ha abierto una nueva sección titulada **"GALDERAK"**, dentro de la cual esperamos poder dar respuesta a las diferentes preguntas que nos puedan llegar sobre diferentes temas relacionados con las Nuevas Tecnologías.

Para todos aquellos que estén interesados en el Boletín y no lo reciban directamente en su buzón de correo o en papel, sabed que también se puede consultar en la **Intranet** del Gobierno Vasco, para lo cual, simplemente se debe acudir a '**Jakina**', y entrar dentro del apartado '**Informática y Telecomunicaciones**'.

Con motivo de estas fechas aprovechamos desde aquí para desearos una feliz entrada al nuevo milenio:

ZORIONAK eta URTE BERRI ON !!

TECNOLOGÍA BLUETOOTH

Se espera que la tecnología Bluetooth sea una revolución en el mercado de las conexiones ya que hace posible las conexiones inalámbricas con todas las ventajas que ello supone.

Es una especificación que permite enlaces de tipo radio de bajo coste entre dispositivos tales como, ordenadores portátiles, teléfonos móviles y otros elementos portátiles. Además permiten que todos estos dispositivos estén conectados a Internet vía radio .

HISTORIA

Bluetooth debe su nombre a un rey vikingo llamado Harald, conocido más tarde como Blatand. El apodo viene de dos viejas palabras danesas, “bla” (oscuro de piel) y “tan” (hombre grande) con lo que los ingleses lo asimilaron fonéticamente como “Bluetooth”.

Desde pequeño, Harald aprendió a respetar los lazos familiares que formaban la sociedad vikinga y a guardarse de los intrusos. Esta filosofía fue lo que decidió a adoptar este nombre a esta nueva tecnología.

Si te interesa ver la Wap del Gobierno Vasco basta con teclear:

euskadi.net (con móvil)

wap.euskadi.net
(emulador de móvil en PC)

BLUETOOTH

Visión General

La tecnología Bluetooth permite realizar conexiones a distancias de hasta 100 metros (10 metros sin amplificadores) y de manera instantánea entre varios dispositivos como por ejemplo teléfonos móviles, agendas y PCs de sobremesa. Todo ello sin usar un solo cable.

Las comunicaciones se realizan mediante transmisión por radio con lo cual, la transferencia de datos y de voz se realiza en tiempo real.

El sofisticado modo de transmisión desarrollado en la tecnología Bluetooth asegura una protección ante interferencias y una seguridad de los datos transmitidos.

El sistema de radio de Bluetooth está construido en un pequeño microchip y opera en la banda de frecuencia de 2,4 GHz accesible en todo el mundo.

La especificación diferencia dos niveles:

- Nivel bajo: Cubre distancias cortas, como la de una habitación.
- Nivel alto: Cubre distancias de rango medio, como por ejemplo la de una casa.

El software controla e identifica el código creado en cada microchip, asegurando que sólo aquellas unidades que estén programadas de antemano puedan comunicarse entre sí.

La tecnología inalámbrica Bluetooth permite comunicaciones punto-a-punto y punto-a-multipunto. Con la especificación actual se ha logrado interconectar hasta 7 dispositivos esclavos con un dispositivo maestro de radio. A este conjunto se le denomina “**piconet**”. Muchos de estos piconet pueden ser enlazados en modo ad hoc (provisionalmente) para permitir comunicaciones entre diferentes configuraciones.

ZUZENKETAK

En la tabla comparativa entre XML/HTTP y JAVA RMI/IIOP de la página 10 de la 1ª edición del Boletín Nº1, se decía que Java es “No orientado a objetos” cuando debía decir “Orientado a Objetos”.

Posibles Aplicaciones

- **Puente a Internet:** La tecnología Bluetooth te conecta al "mundo" desde cualquier lugar en el que te encuentres. Esto hace posible que con un ordenador portátil se pueda navegar por Internet desde cualquier lugar, independientemente si está conectado a un teléfono móvil (tecnología celular) o a través de una conexión por cable (e.j.: ISDN[1], PSTN[2], xDSL[3], LAN[4]).

- **Equipamiento de oficina:** Con esta tecnología todos los periféricos se pueden interconectar de modo inalámbrico. Por ejemplo se puede conectar el ordenador de sobremesa o portátil a impresoras, escaners[5], faxes, ratones y teclados sin los molestos cables. Gracias a esta forma de trabajar, se aumenta la sensación de libertad en el puesto de trabajo.

- **Conferencia interactiva:** En reuniones y conferencias se pueden transferir de forma instantánea documentos a participantes seleccionados e intercambiar tarjetas de negocios electrónicas de forma automática sin necesidad de ninguna conexión por cable.

- **Auriculares**: Los auriculares con esta tecnología pueden "conectarse" a un teléfono móvil, ordenador portátil o a cualquier otro dispositivo y así mantener las manos libres para realizar tareas más importantes en la oficina, en el coche… Mediante el uso de auriculares puedes responder automáticamente a llamadas, activar conexiones con la voz…

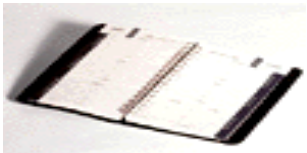
Además de todo eso, los auriculares inalámbricos ofrecen sonido de alta calidad sin que las paredes sean una barrera y permiten la reproducción en audio desde un ordenador portátil. También se pueden controlar tanto el volumen como la ganancia del micrófono.

- **LAN:** Instalando un equipo de trabajo Bluetooth en la oficina, tal y como hemos comentado antes, se eliminarán los tan problemáticos e incómodos cables.

De esta manera se evita el tener que cablear toda una zona para establecer nuevas estaciones de trabajo. Sabiendo que esta tecnología soporta conexiones punto-a-punto y punto-a-multipunto el número de conexiones que soporta virtualmente es ilimitado.

- **Sincronización automática:** Toda la información almacenada en los dispositivos portátiles será accesible desde otros dispositivos con tecnología Bluetooth sin necesidad de cables.

A



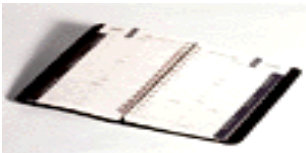
DICCIONARIO

[1] ISDN ó RDSI
(Integrated Services Digital Network). Estándar de comunicación internacional para envío de voz, video y datos sobre líneas de teléfonos digitales o cables de teléfonos normales. ISDN mantiene una velocidad de transferencia de datos de 64 Kbps.

La mayoría de las compañías de teléfono ofrecen dos líneas de una vez. Puedes usar una línea para voz y la otra para datos o puedes usar ambas líneas para datos, lo cual te proporcionará una velocidad de 128 Kbps, tres veces la velocidad de datos proporcionada por los más rápidos módems de hoy.

[2] PSTN
(Public Switched Telephone Network). Sistema de teléfono internacional basado en cables de cobre que transportan datos de voz.

Todo esto en contraste con los más nuevos teléfonos de trabajo basados en tecnología digital. A menudo es conocido como **POTS.**



DICCIONARIO

[3] xDSL
(*Digital Subscriber Lines*). Dos de las principales categorías son ADSL y SDSL.

Las tecnologías DSL usan sofisticados esquemas de modulación para empaquetar datos en cables de cobre. Sólo son usadas para conexiones desde una estación de teléfono a una casa u oficina, pero no entre dos estaciones de teléfono.

[4] LAN
(*Local Area Network*). Conjunto de ordenadores interconectados que comparten recursos, como memoria de almacenamiento, periféricos o aplicaciones.

[5] Escáner
Periférico que convierte información analógica, como páginas impresas o fotos, en valores digitales, con lo que los datos pueden ser almacenados y gestionados desde un ordenador. Otro tipo de escáner son los llamados "escaners dedicados", por ejemplo los que captan información sobre la huella dactilar para identificar a los usuarios válidos de un equipo.

- **Cámaras de video:** La posibilidad de transferir imágenes fijas y video clips entre una cámara y un ordenador portátil es un buen ejemplo de la versatilidad de la tecnología Bluetooth. Cuando la cámara digital es Bluetooth se pueden enviar fotos y videos de forma instantánea desde cualquier lugar sin necesidad de conexión por cable.

- **Conexiones con cable**: La tecnología Bluetooth trata de conectar entre sí diferentes dispositivos digitales mediante conexiones inalámbricas. Para conectarte al mundo necesitas un punto de acceso en tu dispositivo Bluetooth. Cuando estás en "movimiento" este punto de acceso a menudo es el teléfono móvil, cuando estás "quieto" en casa, oficina, hotel… podría ser también una conexión por cable (PTSN[2], ISDN[1], LAN[4] o xDSL[3]).

Independientemente del punto de acceso, todas las conexiones son instantáneas y no se ven interrumpidas por posibles objetos que se pudiesen encontrar entre el emisor y el receptor.

Modelo 3 en 1: En casa el teléfono funciona como un teléfono portátil (línea fija). Cuando estás en "movimiento", éste funciona como un teléfono móvil (línea celular) y cuando tu teléfono entra en la zona de otro teléfono móvil con tecnología Bluetooth, funciona de forma similar a un walkie-talkie.

- **Otros dispositivos electrónicos:** Las previsiones para la tecnología Bluetooth son ilimitadas ya que día a día van apareciendo nuevos productos y aplicaciones así como nuevas funcionalidades para los dispositivos ya existentes. Por ejemplo, escaners[5] y discos duros portátiles, información en los relojes pulsera, centros de refrigeración, máquinas de café, proyectores de presentación,… son sólo unos pocos ejemplos donde la rapidez y la seguridad inalámbrica simplificará nuestra vida diaria.

Velocidad y Seguridad

La tecnología Bluetooth está diseñada para ser totalmente funcional incluso en ambientes muy ruidosos y la transmisión de voz sea audible bajo condiciones muy severas. La tecnología ofrece una alta velocidad de transmisión y los datos están protegidos por métodos de error-conexión avanzados, así como de **encriptación** y **autenticación** para mantener la **privacidad** del usuario.

El ejército francés utiliza la misma banda (2.4 GHz) para sus transmisiones, por lo que los dispositivos de Bluetooth del país galo utilizarán la misma frecuencia pero con saltos a 23 frecuencias, en lugar de 79.

Se espera que para el año 2002, la tecnología Bluetooth esté presente en millones de dispositivos electrónicos.

Dirección de interés:

www.ericsson.com.mx/products/w_data_w_internet/bluetooth/index.shtml

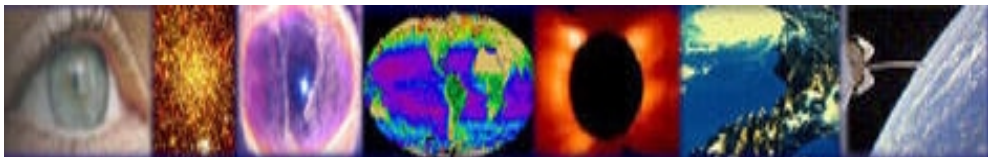
MIGRACIÓN WINDOWS 2000

Win 2K Proffesional es el sistema operativo cliente que sustituye a NT Workstation 4.0.

Win 2K Server es el estándar para los servidores de negocio y sustituye a NT Server 4.0

Win 2K Advanced Server es el que sustituirá a WNT 4.0 Enterprise en grandes redes.

Win 2K Datacenter Server diseñado para tratar con grandes cantidades de datos y procesar transacciones on line.



¿POR QUÉ MIGRAR HACIA WINDOWS 2000?

Durante los últimos cuatro años Windows NT es el sistema operativo más popular de Microsoft para aplicaciones de empresa por la facilidad de servicios que ofrece en el manejo e impresión de archivos desde diferentes departamentos, e-commerce[6] y aplicaciones Web[7].

El argumento más importante para justificar la migración hacia Windows 2000 es la ventaja que suponen las características que este sistema operativo tiene para las empresas:

- Active Directory (Directorio Activo)
- Intellimirror
- Windows Management
- Soporte para usuarios móviles

No hay que olvidar que todo proceso de migración conlleva una serie de cambios e incompatibilidades.

Según Microsoft, de 500 aplicaciones que ha considerado críticas, el 90% sería compatible con W2000, pero, ¿qué ocurre con el 10% restante o con las aplicaciones que ya estaban desarrolladas por las propias empresas?.

- Si se trata de una aplicación de 32 bits que corre en WNT, la probabilidad de que corra en W2000 es de un 99%.
- Si se trata de una aplicación de 16 bits que corre en WNT, la probabilidad de que corra en W2000 es de un 80%.
- Si se trata de una aplicación que corre en Win9x, la probabilidad de que corra en W2000 disminuye con respecto a las anteriores por lo que necesitarán ser reescritas tras la migración.

En el diseño de W2000, Microsoft ha implementado unos cambios, tales como, nuevas estructuras para registros, ficheros y localización de estos últimos con el fin de mejorar con respecto a sus anteriores sistemas operativos en cuanto a confianza y manejabilidad.

DICCIONARIO

[6] e-commerce
Herramientas para la creación de tiendas virtuales.

[7] WEB
Abreviatura de World Wide Web. Conjunto de servidores de Internet que dan acceso a todo tipo de datos, como ficheros gráficos, de sonido o de texto, con referencias (denominadas enlaces o links), a otros documentos en otros servidores.

[8] Cluster
Grupo de almacenamiento, normalmente asociado a un conjunto de sectores dentro de una unidad de almacenamiento.

Ocasionalmente, el sistema operativo marca un cluster usado incluso cuando éste no tiene asignado ningún fichero (esto se llama cluster perdido).

Se puede incrementar el espacio del disco reasignando clusters perdidos pero se debe asegurar primero que estos clusters no contienen valiosos datos.

[9] Microprocesador
Circuito electrónico que contiene la unidad de proceso de un ordenador. Un microprocesador recoge las instrucciones, las descodifica y ejecuta, utilizando sus registros internos y direcciona la memoria externa

A

DICCIONARIO

[10] Interfaz
El elemento que sirve de enlace entre dos dispositivos para asegurar una correcta comunicación de datos. Los más conocidos son la interface paralelo y la serie.

[11] VPN
(Virtual Private Network o Red Privada Virtual). Es una red construida usando cables públicos. Por ejemplo, hay sistemas que posibilitan la creación de redes usando Internet como medio de transporte de información.

Estos sistemas usan la encriptación y otros medios de seguridad para asegurarse de que sólo los usuarios autorizados pueden acceder a la red y que la información no puede ser interceptada.

[12] ISP
(Internet Service Provider) También llamado **IAP**s (Internet Access Providers). Una compañía que da acceso a Internet. El servicio cuenta con un paquete software, una identificación (nombre de usuario) y un password.

Las ISPs también sirven a grandes compañías dándoles acceso directo a Internet.

Entre los ISPs más conocidos están: Airtel, Eresmas, Euskatel, Jazzfre, Navegalia, ...

Mejoras

•**Mejora del rendimiento de las aplicaciones.** El sevicio Windows Management Instrumentation (**WMI**) de W2000 proporciona aplicaciones de más confianza, más accesibles y la habilidad de monitorizar y manejar dichas aplicaciones.

•**Soporte multiusuario y "errante".** Las aplicaciones certificadas por W2000 separarán los usuarios de las máquinas para permitir a los primeros el acceso a sus datos y aplicaciones desde diferentes máquinas y permitirá a diferentes usuarios compartir una misma máquina.

•**Seguridad integrada.** Las aplicaciones certificadas disponen de medidas de seguridad fáciles de manejar y soportan unos procesos de autenticación (single-sign-on) simplificados.

Según los expertos:
- La mayoría de las versiones comerciales de Unix tienen una seguridad muy óptima para trabajar con Internet.
- Linux será el Sistema Operativo más seguro en 2005.

•**Manejo más fácil.** Las aplicaciones accederán a la información común almacenada en el Active Directory para seguridad, políticas, direcciones y otros temas de configuración.

•**Instalación y desinstalación limpia.** Las aplicaciones no dañan las cofigura-

ciones de sobremesa u otras aplicaciones durante el proceso de instalación.

•**Capacidad de explotación de los servicios cluster[8] para disminuir el downtime**. Se da el nombre de downtime al lapso de tiempo de trabajo donde la máquina no es productiva.

¿Qué tipo de seguridad nos traerá Windows 2000?

Microsoft ha diseñado las ediciones Microsoft 2000 Server (servidor) y Professional (sobremesa) para conseguir una plataforma más estable y segura por medio de las siguientes características:

- **Active Directory:** Diseñado para reemplazar los directorios de usuario basados en el dominio de WNT 4.0. Directorio donde se almacenan todos los objetos y recursos de la red en una base de datos jerárquica que puede ser duplicada en cualquier otro punto de la red.

- **Kerberos Versión 5:** Es un protocolo de autenticación estandarizado muy usado en seguridad. Este protocolo fue diseñado para reemplazar a otro protocolo de WNT. Kerberos está muy extendido en las empresas que utilizan Internet y proporciona:

1. Autenticación más rápida
2. Autenticación mutua
3. Extensiones de clave pública
4. Interoperabilidad Win-Unix

- **Soporte para Smart Cards:** Son tarjetas del tamaño de una tarjeta de crédito que incluyen un microprocesador[9], memoria y una interface[10] que hace posible que se pueda trabajar con estaciones de trabajo o redes.

- **Llave Pública:** W2000 está preparado para los innovadores servicios de la criptografía de llave pública (**PK**, Public Key).

- **IPsec:** Es un protocolo de red para la encriptación del tráfico **TCP/IP**. Abarca tres áreas de seguridad: autenticación, integridad de datos y privacidad de datos.

- **Sistema de ficheros NT mejorado: NTFS** (NT File System) ha sido mejorado para incorporar las funciones de encriptación.

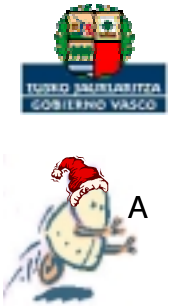
- **Mejora del soporte para las Redes Privadas Virtuales (VPN[11],** Virtual Private Network**):** Ofrece nuevas herramientas para facilitar la administración de las VPNs, como por ejemplo, el proceso de establecimiento de conexión entre el usuario y el servidor. Igualmente permite a los Proveedores del Servicio de Internet (**ISP[12]**, Internet Service Providers) y a los administradores del sistema establecer una conexión a Internet de rápido acceso.

El Gobierno Vasco tiene pensado en breve migrar a W2000 todos sus servidores

Direcciones de interés:

http://enete.us.es

http://www.microsoft.com/spanish/windows2000



	WNT 4.0	WINDOWS 2000
CAPACIDAD	Soporta hasta 40.000 usuarios por dominio	Soporta hasta 10 millones de objetos que representan los recursos de la red, como usuarios, equipos e impresoras
COPIA	Sólo el controlador del dominio primario (Maestro) puede leer y escribir en la base de datos del dominio. Los cambios son duplicados en los controladores del dominio Backup.	Multimaster - Todos los controladores de dominio tienen una copia de la base de datos del dominio.
RESOLUCION DE NOMBRES IP	Servicio Windows de Nombres de Internet (WINS, Windows Internet Naming Service)	Servidor DNS (Domain Name Server)
NOMBRES DE DOMINIO	Nombres de la NetBIOS.	Nombres de dominio DNS

GALDERAK

¿Qué es Java RMI/IIOP?

- **RMI** (Remote Method Invocation) Es una tecnología propia de programación distribuida orientada a objetos totalmente basada en Java. La idea básica de esta tecnología es que, objetos ejecutándose en una VM (Virtual Machine) sean capaces de invocar métodos de objetos ejecutándose en VM´s diferentes. Haciendo notar que las VM´s pueden estar en la misma máquina o en máquinas distintas conectadas por una red.

- **IIOP** (Internet Inter-ORB Protocol) Especifica un protocolo estandarizado para la interoperabilidad en Internet, permitiendo interoperar con otros ORB´s compatibles basados en los productos más populares.

- **MIDDLEWARE** Software que conecta dos aplicaciones diferentes.

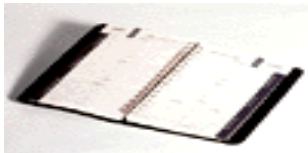
- **ORB** (Object Request Broker) Componente que actúa como middleware entre clientes y servidores.

SEGURIDAD EN EL CORREO ELECTRÓNICO

A

Es bien conocido por todos que hoy en día no existe un sistema computarizado que garantice al 100% la seguridad de la información debido a la inmensa mayoría de diferentes formas con que se puede romper la seguridad de un sistema.

Sin embargo, una buena planificación de la estrategia para dar seguridad a la información puede resultar la salvación de una empresa.



DICCIONARIO

[13] DES
(Data Encryption Standard, estándar de cifrado de datos). Es un algoritmo desarrollado originalmente por IBM bajo el nombre de Lucifer, como estándar de cifrado de todas las informaciones sensibles no clasificadas.

DES cifra bloques de 64 bits, mediante permutación y sustitución, para lo cual usa una clave de 64 bits, de los que 8 son de paridad.

[14] RSA
(Rivest, Shamir and Adelman, inventores de la técnica). El algoritmo RSA está basado en el hecho de que no hay camino eficiente para factorizar números muy largos.

Por ese motivo, deducir una clave RSA requiere una extraordinaria cantidad de ordenadores y tiempo.

El algoritmo RSA se ha convertido en el estándar de encriptación para industrias fuertes, especialmente para enviar datos a Internet. Está basado en muchos productos software, incluyendo Netscape Navigator y Microsoft Internet Explorer.

La tecnología es tan poderosa que el Gobierno Americano ha restringido su exportación a países extranjeros.

DES es más rápido que RSA por lo que se utiliza más en Internet y comercio electrónico.

CRIPTOGRAFÍA

La palabra criptografía proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, "escritura escondida".

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar[15] o encriptar). A continuación manda el mensaje por una línea de comunicación que se supone "insegura" y después sólo el receptor autorizado podrá leer el mensaje "escondido" (lo llamamos descifrar o desencriptar).

La criptografía se divide en dos grandes ramas: la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica.

Origen de los ataques:
Un "hacker" independiente, un 34.74%
Un competidor, un 24.88%
Un empleado disgustado, un 40.33%

CRIPTOGRAFÍA SIMÉTRICA

La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar, de tal modo que sólo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar el mensaje.

Presenta el inconveniente de que para utilizarse en comunicaciones, la clave debe estar tanto en el emisor como en el receptor, lo cual nos lleva a preguntarnos cómo transmitir la clave de forma segura. El sistema criptográfico simétrico más conocido es el llamado **DES**[13].

CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica utiliza dos claves diferentes para cada usuario, una pública, conocida por el resto de usuarios y que usarán para cifrar los mensajes dirigidos al propietario de ésta, ó para descifrar/comprobar la firma del mismo, y otra privada, utilizada para descifrar los mensajes recibidos (encriptados con la clave pública) y para firmar sus propios mensajes. El **RSA**[14] es el más utilizado dentro de los sistemas asimétricos.

En la práctica se emplea una combinación de estos dos tipos de criptosistemas, ya que el segundo presenta el inconveniente de ser tecnológicamente mucho más costoso que el primero.

Hasta hace 25 años el intercambio de mensajes cifrados era un privilegio de militares, diplomáticos y servicios secretos.

El lanzamiento del popular programa **PGP (Pretty Good Privacy)** en 1991, hizo por fin realidad el acceso de las masas a las ventajas del correo electrónico ultraseguro.

En el mundo real se codifican los mensajes (largos) mediante algoritmos simétricos que suelen ser muy eficientes y luego se hace uso de la criptografía asimétrica para codificar las claves simétricas (cortas).

¿QUÉ ES PGP?

PGP (Pretty Good Privacy, "intimidad bastante buena") es el paquete de seguridad desarrollado por Phil Zimmermann más extendido y acreditado para el cifrado del correo electrónico tanto para Internet como para X.400. Utiliza 128 bits.

El utilizarlo equivale a dotar al correo electrónico de los valores añadidos:

- Confidencialidad[16]
- Autenticación[17]
- Integridad[18]

¿Qué versión de PGP se debe utilizar?

Son dos las versiones internacionales más importantes: 2.6.3i y 5.0i. Entre ambas hay varios años de diferencia y un salto cualitativo importante siendo la versión 5.0i la más moderna y fácil de usar.

La versión 2.6.3i a pesar de ser potente y fiable no era fácil de utilizar debido a la carencia de una interfaz gráfica adecuada.

La versión 5.0i proporciona al usuario la posibilidad de elegir entre diferentes algoritmos de cifrado simétrico o asimétrico.

FIRMAS DIGITALES

¿Qué son?

Es un bloque de caracteres que acompaña a un documento, acreditando quién es su autor (**autenticación**) y que no ha existido ninguna manipulación posterior a los datos (**integridad**).

¿Cómo se realizan?

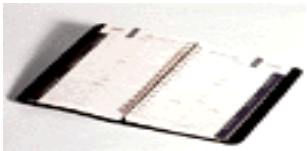
El software del firmante aplica un algoritmo hash[19] ("revoltijo") sobre el texto a firmar, obteniendo un extracto de longitud fija, y específico para ese mensaje (Un mínimo cambio en el mensaje produce un extracto completamente diferente).

¿Cómo se comprueba la validez de una firma digital?

El software del receptor descifra el extracto cifrado que constituye la firma digital utilizando para ello la clave pública del remitente. Como resultado obtiene un bloque de caracteres.

Después, calcula el extracto hash que corresponde al texto del mensaje. Si ambos textos coinciden, la firma se considera válida, pero si existe la menor diferencia, se considera no válida.

Los usuarios intercambian certificados unos con otros sin necesidad de utilizar entidades de certificación



DICCIONARIO

[15] Cifrar
Tomar un mensaje normal legible (texto en claro) y convertirlo en un revuelto de caracteres ininteligible a simple vista (texto cifrado).

[16] Confidencialidad
Asegura que ningún extraño pueda leer el correo

[17] Autenticación
Es el proceso de identificar un individuo basándose en el nombre de usuario y password. La autenticación asegura que un inviduo es quien dice ser pero no da ninguna información sobre los derechos de acceso de ese individuo.

[18] Integridad
Asegura que no se ha producido ninguna manipulación efectuada por terceros sobre los mensajes o ficheros enviados o recibidos.

[19] Hash
Es una función de un solo sentido que asocia un archivo o documento de longitud arbitraria a una cadena de longitud constante (se usa actualmente 160b de salida), las funciones hash más conocidas son: MD5, SHA1, RIPMED 160.

A

¡¡BREVES!!

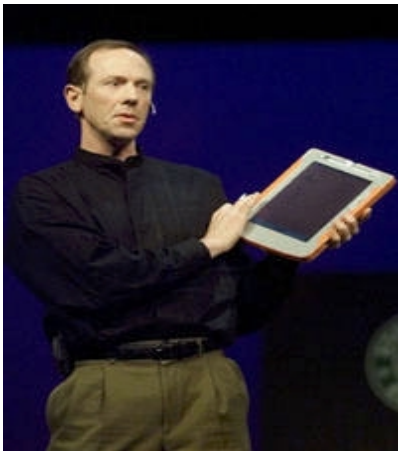
Tablet PC de Microsoft

El nuevo aparato de Microsoft es un poco más grande que una PDA (Personal Digital Assistant) y almacena notas escritas a mano que después se pueden manipular electrónicamente.

El Tablet PC que posiblemente llegará a las tiendas en el año 2002 parece a primera vista un simple reproductor de notas; pero una vez registradas, se pueden editar, modificar e incluso realizar búsquedas por palabras.

Tablet PC tendrá el tamaño de un folio y será más ligero que un ordenador portátil. Tendrá una gran utilidad cuando estemos fuera del despacho, cuando nos encontremos en alguna reunión…

"El Tablet PC me permitirá estar el doble de horas desconectado del ordenador" afirmó Bill Gates.



La nueva terminal funcionará con el sistema operativo Whistler de Microsoft (actualmente en fase de pruebas) y podrá incorporar teclado, ratón y un suplemento de memoria RAM. Pero, la gran ventaja será que las notas escritas a mano tal y como se ha comentado anteriormente, podrán ser formateadas por palabra, frase o párrafo, de la misma forma que sucede en un procesador de textos.

Por supuesto, el Tablet PC tendrá el sistema más avanzado de reconocimiento de escritura, aunque no se hizo ninguna demostración del sistema durante la presentación que tuvo lugar el 12 de Noviembre en la Feria Informática Comdex en Las Vegas. Un portavoz de Microsoft aseguró que, cuando el aparato llegue a la calle, esta tecnología irá incorporada.

Durante el año pasado se investigó cómo hacer que diferentes terminales informáticas interactúen entre sí (y de ese modo permitir al consumidor utilizar el mismo documento desde diversos aparatos.)

ACCESO AL TRABAJO MEDIANTE LA VOZ

Las interfaces de voz cambiarán la manera de utilizar los Sistemas Informáticos. Se podrán dictar textos y controlar el ordenador con la voz con mayor precisión y comodidad.

Así mismo permitirá controlar la Web mediante la voz, con lo que podremos navegar, crear y enviar mensajes de correo electrónico.

Interfaces de voz

Internet ha supuesto una revolución en la manera de gestionar los servicios al cliente. Para ser competitivo en el mundo del e-business, las compañías deben simplificar y mejorar su interacción con los usuarios facilitándoles el acceso a la información independientemente del lugar y hora en que se encuentren.

Los usuarios cada vez demandan más la capacidad de acceder a la información de una forma personal y de realizar las transacciones a su conveniencia. Esta tendencia requiere que las compañías ofrezcan una manera sencilla de trabajar por lo que las interfaces de acceso a la información tienden a ser cada vez más **naturales**.

La demanda de acceder a la información a cualquier hora y desde cualquier lugar está empujando a que el acceso a Internet sea cada vez más común realizarlo desde dispositivos móviles. Es por ello que los teléfonos y otros dispositivos son cada vez más numerosos y los teclados de dichos dispositivos cada vez más pequeños.

Así, la tecnología de la voz será cada vez más importante en el diseño de las interfaces de usuario para el acceso a la información.

Las tecnologías del lenguaje humano incluyen nuevas funciones en los ordenadores como por ejemplo:

- **Reconocimiento de voz**
- **Sintetizadores de voz** que se incluyen en los sistemas conversores de texto a voz

APLICACIONES

1. Utilizar los comandos de lenguaje natural para decirle al sistema lo que se desea hacer, por ejemplo crear, editar y corregir correspondencia, formularios y otros documentos de forma fácil.

2. Usar plantillas activadas con la voz para documentos con formato estándar, tales como presupuestos.

3. Utilizar métodos abreviados de voz (macros) para insertar texto que se utiliza con frecuencia, como direcciones y párrafos estándar. Con lo que se consigue ahorrar tiempo.

4. Hablar para abrir y cerrar aplicaciones, cambiar el tamaño de las ventanas en la pantalla.

5. Navegar por la Web y gestionar su correo electrónico.

6. Dictar directamente a Internet Explorer, Netscape y programas de Chat para crear correo y mensajes instantáneos.

7. La función texto-a-voz ofrece la posibilidad de leer en voz alta el correo electrónico, páginas Web y otros documentos.

Direcciones de interés:

www.hj.com/JAWS/JAWS37.htm

www.hj.com/NewsCommentary/Adaptive.html

ALBOAN: EJIE
TARJETA DE SEGURIDAD
PKI

OBJETIVOS

Define la implementación de la PKI en las aplicaciones del Gobierno Vasco

Se refiere a la implantación de las políticas, estándares y servicios que hacen posible que una comunidad de usuarios puedan comunicarse dentro de un marco de confidencialidad, autoría, **integridad** y **no repudio** a un mensaje o transacción. Así, todos los trámites de la empresa se podrán realizar a través de Internet de forma segura gracias a la PKI (Public Key Infraestructure).

CARACTERÍSTICAS

La longitud de la clave es de 1024 bits y se instalará el Internet Explorer 5.01 . El lector de la tarjeta va conectado en serie con el ratón.

Correo Gobierno Vasco

La institución utiliza Exchange como servidor de correo.

Se enviará acuse de recibo entre los servidores Exchange.

Se validarán desde Outlook las CRLs (Client Revocation List, Lista de Revocación de Usuarios).

Se publicarán las claves públicas de cifrado en el directorio de Exchange.

EJEMPLO

Proyecto piloto de INTEK:

Se trata de permitir la Tramitación Telemática de Solicitud de Ayudas en el Área de Promoción a la Investigación y Desarrollo Tecnológico de las Empresas. Está integrado dentro del proyecto e-delfos del Dpto. de Industria.

Aplicación Web desarrollada en Java con servidor de aplicación Weblogic.

El pasado martes día 12 de Diciembre, el proyecto PKI del Gobierno Vasco fue aprobado en Consejo de Gobierno.

Más información en: http://www.ej-gv.es/intek