SKYSOFT

SKYSOFT SERVICIOS S.A.

ANEXO I

SISTEMA DE MENSAJERÍA MILITAR ELECTRÓNICA SEGURA (MMHS)

DESCRIPCIÓN TÉCNICA GENERAL

Índice General

I Introducción y conceptos generales

II Funciones del sistema

III Estructura del sistema

IV Cumplimiento de los Protocolos X.400/X.500

V Soporte Técnico

I. INTRODUCCIÓN Y CONCEPTOS GENERALES

Skysoft Servicios S.A. (SKYSOFT) ofrece una solución probada y completa para un Sistema de Mensajería Militar Electrónica Segura (MMHS). El sistema es capaz de interconectar los usuarios ubicados ya sea localmente, interconectados mediante una LAN, así como también los usuarios remotos del interior del país, utilizando los vínculos existentes. El sistema incluye la totalidad de los medios materiales nuevos y recursos humanos para asegurar el correcto funcionamiento, durante las 24 horas. El sistema tendrá una confiabilidad anual que supera el 99,999%.

El Sistema de Mensajería Militar Electrónica Segura (MMHS) responde a los estándares definidos por la Unión Internacional de Telecomunicaciones (UIT) en conjunto con las normas de la International Standard Organization (ISO), International Electrotechnical Commision (IEC) y respondiendo totalmente a la estructura de transmisión de correo electrónico X.400.

Los mensajes, que cumplen con el formato P722, se enviarán a un conmutador de mensajes MTA/MS, desde donde se enrutarán a sus destinos. Si estos destinos son otros usuarios X.400 pertenecientes al dominio, se transmitirán usando los protocolos X.400 P3 al MS y luego serán recibidos por las Terminales utilizando X.400 P7, mientras que serán encaminados con protocolos X.400 P1 para dirigirlos a un MTA adyacente.

Nuestra solución hace uso de un MTA/MS/DS basado en equipos COTS y software X.400/X.500 LDAP COTS. Asimismo el mismo producto de mensajería X.400 se utiliza en los 73 lugares y 200 terminales del sistema AMHS de Argentina, en operación desde diciembre de 2005, tramitando diariamente 65.000 mensajes, como también la Prefectura Naval y la Fuerza Aérea Argentina. Nuestros diseñadores

cuentan con la disponibilidad de las funciones más modernas de los distintos productos COTS, y ellas se incorporarán en cada solución del Sistema de Mensajería Electrónica Segura ofrecida.

Se considera importante disponer de la facilidad que tendrá el sistema para operar integrando todos los recursos técnicos que ofrece nuestra solución.

Todo el equipamiento se conectará a la red de energía comercial 220 VCA 50Hz.

Nuestro producto de Sistema de Mensajería Electrónica Segura cumple con aquellas indicadas para el servicio de mensajería, incluyendo:

- Directorio que permite realizar una configuración dinámica.
- Soporte del Directorio para el mapeo de direcciones, páginas públicas, soporte de seguridad a través de PKI y herramientas para gestión de datos.
- Enrutamiento del Sistema de Mensajería Electrónica Segura SKS X400, basado en el uso de X.500 para contener el esquema general y X.400 para efectivizar la asignación de rutas.
- MTA y MS que cumplen los requisitos del Servicios de Mensajería Electrónica Segura.
- Administración del Sistema con todas las funcionalidades requeridas.

Capacidades y funcionalidades básicas del Sistema:

Las principales capacidades y funcionalidades son:

- Creación de un ambiente adecuado para una transición de los actuales sistemas.
- Enrutamiento incluyendo soporte a Directorio (extendido usando listas de distribución).
- Re-enrutamiento automático de mensajes.
- Archivo (mensajes, registros, estadísticas y alarmas).
- Recuperación de mensajes.
- Estadísticas.
- Comunicación con usuarios locales (sobre protocolos ITU-T X.400, P7 ó P3).
- Posibilidad de conversión de dirección y formatos. (Opcional)
- Configuración dinámica
- Monitoreo del MTA/MS/DS.
- Agente SNMP para administración de redes.
- Mensajes generados sin restricción de longitud, ni destinatarios.

- Almacenamiento de todo el tráfico, reportes, estadísticas, logs, etc., al menos de los últimos treinta (30) días.
- La información guardada en medios magnéticos externos podrá ser recuperada para propósitos legales o en caso de desastres.

La operación del sistema se realiza mediante GUI, en caso que se desee ingresar comandos del tipo texto en el sistema operativo, estos se comportan de manera estándar Unix con respuesta inmediata e información de estado y/o ayuda en línea al instante.

Funcionalidades extendidas:

- Reconocimiento real de entrega de mensajes de extremo a extremo.
- Tamaño del mensaje de longitud ilimitada.
- Contenido del mensaje no limitado a texto exclusivamente (binario, codificado, gráfico, etc.).
- Tres niveles reales de prioridad de acuerdo a normativa X.400.
- Vencimiento de mensajes de acuerdo a lo establecido en la normativa X.400.

Consideraciones de diseño: el sistema está diseñado basado en el modelo de arquitectura cliente-servidor y en el modelo de referencia de Interconexión de Sistemas Abiertos OSI.

La arquitectura es totalmente modular, basada en diversos servicios de aplicación que corren en el servidor

Constitución del sistema: el sistema está basado en los siguientes sistemas operativos:

- Windows 10 ó superior para los Terminales.
- Linux Red Hat Enterprise: para los servidores del MTA/MS/DS Los sistemas se integran en base a los siguientes componentes:
- M-Switch MTA/MS (Servidores de Mensajería ATS X.400).
- M-Vault DS (Servidores de Directorio X 500).
- Aplicaciones para Administración y Supervisión.
- Terminales Sistema de Mensajería Electrónica Segura SKS X400.
- WAN sobre TCP/IP (no incluido en el alcance de esta propuesta)

Estas características técnicas permitirán, mediante la concreción a las redes WAN y LAN, establecer la comunicación con las terminales que se prevean.

II. FUNCIONES DEL SISTEMA

CONMUTACIÓN SISTEMA DE MENSAJERÍA ELECTRÓNICA SEGURA

MESSAGE TRANSFER AGENT (MTA)

Nuestro MTA actual está basado en el producto comercial M-Switch X.400.

El M-Switch X.400 es una aplicación de alto rendimiento, siendo un Agente de Transferencia de Mensajes (MTA) X.400 muy flexible y robusto. Es conveniente para ser usado como un MTA departamental o principal, y soporta el uso de listas de distribución.

M-SWITCH X.400

El M-Switch tiene muchas funciones, las que se describen a continuación:

La flexibilidad de la arquitectura del M-Switch X.400, así como las herramientas de administración y las aplicaciones propias, se combinan para dar un alto grado de posibilidades para el cliente. El M-Switch X.400 es una opción ideal comparada con otros productos COTS que proporcionan menos posibilidades, y no pueden llenar los mismos requisitos.

Conformidad con los Estándares: Es poseedor de servicios que cumplen absolutamente con los protocolos X.400 basados en un servidor que es compatible / operable con todas las series de servidores X.400. Este cumplimiento se encuentra certificado a través de documentos llamados “Protocol Implementation Compliance Statements” o PICS de acuerdo a la normativa ISO.

Mantiene una compatibilidad absoluta con los servicios de Directorio X.500.

Excelencia en su planificación y características operacionales: el Administrador de Cola de Mensajes (QMGR) y la arquitectura de canales descripta en el apartado correspondiente, permite una sofisticada planificación, que combinada con la estructura del Administrador de cola de Mensajes, ofrece un producto que trabaja perfectamente en ambientes operativos de alta exigencia.

Configuración basada en Directorio: el M-Switch X.400 usa un Directorio de LDAP/X.500, accedido por X.500 DAP o CLDAP de altas prestaciones. Este es de hecho el mecanismo de configuración preferida.

Administración de Interfaz Gráfica de Usuario (GUI) configurable: la administración del GUI usa el lenguaje Tcl scripting. Este hace que las herramientas de administración sean muy flexibles y accesibles para las aplicaciones de administración.

Características de Gestión: el producto tiene una amplia gama de servicios de administración, incluyendo la configuración, supervisión SNMP, listas de distribución, contenido de conversión y control sobre el mapa de direcciones.

El mapa de direcciones contiene sofisticados servicios para habilitar la transformación de las direcciones de correo. Esta característica es particularmente útil al tratar con sistemas dispares que necesitan ser integrados en un sistema amplio y coherente.

Seguridad: existe una variedad de rasgos de seguridad, incluso los mecanismos de seguridad propios de X.400 y un control de autorización para mensajes de propósito general.

Verificación de virus sobre mensajes X.400: una característica muy flexible que permite el uso de diferentes antivirus para verificar los paquetes procesados. Esto se provee como un producto adicional en caso de que sea requerido por el usuario.

Seguimiento de mensajes: La funcionalidad de seguimiento o rastreo de mensajes. Los mensajes pueden buscarse en base a parámetros típicos para el supervisor, como ser: tiempo de llegada, creador del mensaje, destinatario y asunto. Esta clase de interfaz de búsqueda confiere excelente flexibilidad para recuperar mensajes. Para cada solicitud, el sistema proporciona un informe con el resultado correspondiente en el puesto del supervisor. Los mensajes seleccionados como resultados de la búsqueda, se visualizan en el puesto del supervisor. El supervisor puede reinsertarlo como un nuevo mensaje.

MESSAGE STORE (MS)

Nuestro MS está basado en el producto M-Store X.400, que soporta X.400 P7 para comunicarse con las Terminales y utiliza X.400 P3 para conectarse a un MTA, tal como el M-Switch X.400. Sirve como intermediario entre los Agentes Usuarios (AU) y el Agente de Transferencias de Mensajes (MTA), al aceptar la entrega de mensajes en nombre del usuario y guardarlo para una subsecuente recuperación por parte del AU. El MS también mantiene un servicio de envío indirecto y facilidades de búsqueda, listado y tratamiento de mensajes.

Beneficios clave: los mayores beneficios que proporciona el Almacén de Mensajes X.400 son:

El M-Store X.400 es un producto robusto, e incluye soporte a tecnología Fault Tolerance.

El uso de MS permite asegurar la disponibilidad de mensajes aún cuando temporariamente se encuentren deshabilitados vínculos o terminales, quedando disponibles para cuando se reinicie el servicio. Esto permite asegurar un 100% de disponibilidad del servicio. Básicamente se funda en la posibilidad de que el MS retenga hasta la entrega aquellos mensajes que no son extraídos inmediatamente por los AU. El volumen de mensajes a almacenar sólo depende del hardware asignado al M-Store.

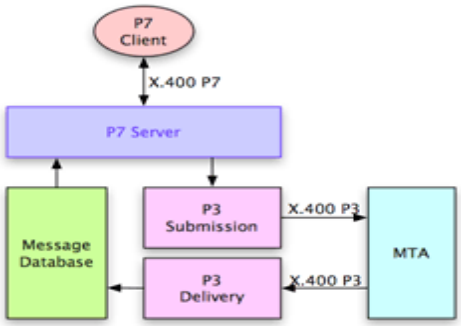
El uso de mensajería basada en configuración sobre Directorio X.500 da mucha flexibilidad de operación, integrando el M-Switch y el M-Store. Esta facilidad se maneja con interfaz gráfica o de scripting.

El MS brinda soporte al uso de protocolos P3 y P7.

El Almacén de Mensajes no necesita estar localizado junto con el conmutador de mensajes ni requiere un MTA dedicado, lo que significa que un simple M-Switch puede soportar muchos almacenes de mensajes. Esta característica da un alto grado de flexibilidad.

Arquitectura: El diagrama siguiente ilustra la arquitectura del almacén de mensajes (MS) X.400 y su relación con el cliente, basada en P7 y con el MTA X.400 basada en P3. La clave del MS es su API interna, que define una abstracción de la base de datos del MS.

De este modo se configura también un soporte a la Mensajería Interpersonal X.400 dónde los protocolos P2/P22 se encuentran especificados. El diseño de la base de datos permite el acceso por múltiples protocolos: P7 y P3.



El almacén de mensajes tiene varios componentes:

Un motor de base de datos diseñado para el M-Store X.400, construido en base al almacén de archivos subyacentes.

Un proceso de servidor que usa un motor de base de datos para dar un servicio de almacenamiento de mensajes X.413/X.420.

El M-Switch X.400 se despliega como un solo proceso que puede soportar a múltiples conexiones P3 y P7. El número de usuarios y casillas de correo sólo estará limitado por la capacidad del hardware. A modo de ejemplo, se encuentra operativo un sistema diseñado, instalado y puesto en servicio por nuestra empresa con más de 3.000 casillas de correo y con altos requerimientos de seguridad.

Soporte a X.400: el MS soporta X.400 utilizando el protocolo P7 del X.400 para dar soporte a los usuarios clientes de sus casillas de mensajes. Esto permite la recuperación de mensajes.

El MS soporta envíos y entregas del MTA usando el servicio X.411 (protocolo P3). Esto proporciona una posición de independencia del MTA con respecto a los destinatarios y aumenta al máximo su funcionalidad. El P3 puede configurarse para obtener envío y entrega sobre la misma asociación o por sobre asociaciones separadas.

Administración:

Para la administración y management de los productos de software COTS servidores, el sistema cuenta con sendas aplicaciones GUI cliente-servidor que se conectan al servidor mediante TCP/IP permitiendo realizar con facilidad tareas de administración tanto local como remota, entre ellas creación y configuración de MTAs, MS, UA´s (Mailboxes) y Management general del directorio en forma rápida, sencilla y amigable.

El uso de Directorio para la configuración del MS da mucha flexibilidad, a la par que facilita integrarla con la configuración del M-Switch. De este modo se permite la administración simultánea de la configuración cliente/servidor y compartir información de configuración entre servidores. La configuración se maneja con una interfaz gráfica.

SERVIDOR DE DIRECTORIO (DS)

El servidor del Directorio está basado en el M-Vault X.500, producto comercial (COTS) que proporciona servicios al MTA y a los agentes de usuario.

El Servidor X.500 es un servicio de Directorio de alto rendimiento que puede ser accedido mediante protocolos DAP (Directory Access Protocol) LDAP (Lightweight Directory Access Protocol).

Soporta X.500:

- DAP (*Protocolo de Acceso a Directorio*)
- DSP (*Protocolo de Sistema de Directorio*) y
- DISP (*Protocolo de Replicación –Shadowing- de Información de Directorio*).
- A través del encadenamiento o “chaining” entre servidores establecido en la normativa X.518, nuestros servidores se integran en un directorio global.

M-Vault puede usarse como un servicio X.500 autónomo e independiente, o simplemente para dar soporte en cuanto al rutea del MTA. Tiene funcionalidad total X.500 (1993) que incorpora la replicación, el control de acceso, la autenticación estricta y otros rasgos de seguridad.

El soporte integrado LDAP soporta su uso como un servidor de Directorio X.500, como servidor de Directorio LDAP, o ambos. Esta flexibilidad permite a una organización el uso de LDAP y clientes de DAP X.500.

M-Vault X.500 usa replicación X.500, control de acceso y facilidades de administración para construir un servicio troncal (backbone) muy funcional, seguro y de apertura genuina. Los servidores de terceros que soportan LDAP, pero no X.500, también pueden llegar a integrarse a esta infraestructura de la red.

Entre muchas razones por las que el M-Vault X.500 resulta ser la opción correcta para proveer servicios de Directorio se incluyen:

- Soporte directo para LDAP, habilitando el soporte eficaz de clientes LDAP y de aplicaciones habilitadas para LDAP.
- Muy alto rendimiento para la lectura, funciones de búsqueda y de modificación combinadas con un alto nivel de escalabilidad para Directorios que contienen millones de entradas.
- Soporte total para funcionalidad X.500 en el servidor y bibliotecas del cliente, funcionalidades X.500.
- Provee una estructura de trabajo (framework) para el back-end de un Directorio distribuido que usa X.500, lo que lo convierte en el único producto independiente disponible para la venta. Se describen los beneficios de este sistema en la publicación llamada “Building and Enterprise Directory using LDAP and X.500”.
- Funcionalidad flexible de replicación escalable que usa X.500 DISP (Protocolo de Replicación –Shadowing- de Información de Directorio).
- Subsistema de transacción de bases de datos de primer nivel que proporciona la seguridad de que el hardware, el sistema operativo o fallos de la aplicación no adulterarán el banco de datos del servidor de Directorio. Este soporte para transacciones también permite los procedimientos de resguardo en línea para casos de recuperación luego de una caída.
- Soporte a SSL/TLS. La seguridad entre el cliente y el servidor del Directorio se proporciona por SSL/TLS preparando una sesión segura entre los dos extremos y permitiendo la criptografía e integridad de datos en el enlace. Adicionalmente, SSL/TLS pueden ofrecer autenticación optativa del servidor, o del cliente y del servidor.
- Encadenamiento de LDAP. Esto promueve la interoperabilidad con servidores sólo LDAP y con todos los clientes que poseen integración eficaz con los servidores de LDAP dentro de un ambiente de servidores distribuidos.
- Multiprotocolo de alto rendimiento, arquitectura multitarea escalable para plataformas multiprocesador con posibilidad de extensión para fácil soporte de protocolos adicionales. Da soporte a SMP (Multiprocesamiento Simétrico) para aprovechar el poder de sistemas de multiprocesamiento como los servidores integrados en nuestra solución.
- Monitoreo por SNMP utilizando Administración de Mensajería y Directorio por Internet (MADMAN) según especificaciones (RFC 2248 y RFC 1567). No es usada en nuestra solución. Por considerarla no segura
- Las características de seguridad ofrecen control de acceso X.500, autenticación estricta X.509, configuración y control de la política de seguridad.
- Configuración avanzada y herramientas de administración, incluso herramientas de carga y de volumen que vienen como una parte del Servidor

M-Vault. Estos permiten desplegar y administrar fácilmente el servidor en una amplia gama de Intranets y ambientes de Extranet.

- La funcionalidad de Administración de Índice Dinámico permite agregar y eliminar índices, mientras el servidor de Directorio está corriendo, permitiendo disponibilidad de 24 hs. x 7días.

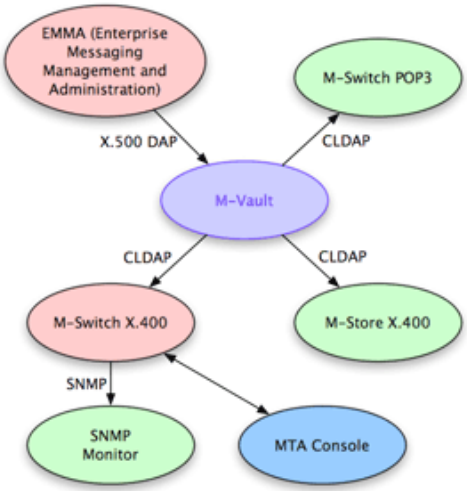
Seguimiento de información estadística disponible: el sistema permite realizar una variada y completa estadística del sistema, mediante un sencillo parámetro seleccionable (día, mes, año, desde / hasta).

- Disponer del total de mensajes entrantes y/o salientes, medidos por hora, por día, por semana, por mes para un determinado MTA.
- Cantidad de caracteres entrantes y/o salientes, medidos por hora, por día, por semana, por mes para un determinado MTA.
- Estadística horaria, diaria, semanal, mensual, de mensajes rechazados y/o puestos en cuarentena para un determinado MTA.
- Promedio, mediana y 90% de latencia por hora, por día, por semana, por mes por mes para un determinado MTA.
- Combinación de las estadísticas anteriores o combinación de MTA.
- Sumarios mensuales (total entrantes, entregados localmente o transferidos)
- Individuales por mailbox medidos por hora, por día, por semana, por mes.
- Top 10 y 100 Originadores y Recipientes

Para post procesar la información estadística, desde MS EXCEL® pueden importarse directamente los datos tomando como fuente las bases de datos estadísticas del sistema.

FACILIDADES DE ADMINISTRACIÓN

En el siguiente diagrama se muestran los principales componentes del sistema de administración de mensajes, con flechas que muestran el flujo de la información administrativa.



La herramienta de administración primaria es la llamada Administrador de Mensajería Institucional (MConsole) que permite administrar la configuración de toda la mensajería perteneciente a un dominio de organización. La configuración del Sistema de Mensajería Electrónica Segura SKS X400 se representa en el Directorio, el cual otorga el beneficio de compartir la información de configuración entre servidores y facilita la administración cliente / servidor.

El sistema cuenta con absolutamente todas las posibilidades de ser operado por medio de aplicaciones gráficas, que se ejecutan en las consolas de supervisión y no es necesaria la introducción de comandos de tipo texto para operar/supervisar el sistema. Consideramos que este es el modo natural de uso que supera los requerimientos del pliego licitario.

Sólo para el caso del sistema operativo servidor (Linux RedHat) podrá o no utilizarse la interfaz gráfica que posee o bien optar por introducir comandos nativos del S.O. (comandos Unix estándar) para cuyo uso se puede recurrir a la ayuda estándar que el S.O. ofrece, abundante y muy accesible.

Además de las posibilidades auxiliares de realizar la copia de respaldo de la configuración para uso posterior o modificación de la misma, el uso de una serie de medios redundante y común de un conjunto de discos permite que al cambiar los servicios o hardware de soporte, los archivos de configuración no necesiten ser reconfigurados.

Configuración del Directorio basada en tablas o en el Directorio

Los productos de mensajería tienen dos paradigmas básicos para la administración de la configuración.

Basados en tablas. La configuración se especifica en un juego de tablas de texto y mediante un texto “a medida”. Esto se describe en los manuales del producto, y da soporte a todos los productos, excepto el M-Store X.400.

Basados en Directorio. La configuración se especifica completamente en el Directorio.

Ambos tipos de operación tienen ventajas, y se continuará apoyando ambos. En general, recomendamos y utilizamos el uso de la configuración basada en el Directorio. La configuración basada en tablas es normalmente apropiada para situaciones especiales (por ejemplo, para configuraciones extremadamente sencillas).

La configuración basada en el Directorio constituye un poderoso avance, ya que permite una visión panorámica de la configuración de una organización. La información redundante es compartida entre los servidores y se permite la administración segura y eficiente de cliente / servidor. Esto significa una vía ilimitada de acceso a los servicios de configuración.

Beneficios clave de la configuración basada en el Directorio

Proporciona varios beneficios:

- Permite amplia visión de una organización. El acceso integrado a la administración de la configuración permite que la operación de un servicio de mensajería tenga una visión coherente total de la empresa, o sea, el proceso se realiza a la inversa de trabajar para administrar un grupo de servidores tratando la configuración de cada servidor en forma individual.
- Eliminación de información redundante. La configuración basada en Directorio permite compartir información entre servidores disminuyendo la redundancia y el exceso de trabajo de administración.
- La administración de Cliente/Servidor. El uso de Directorio permite administrar en forma segura y eficiente la configuración cliente/servidor, lo que permite verdaderamente manejar la configuración desde cualquier lugar.
- Herramientas gráficas y de scripting. Las herramientas de administración están disponibles con interfaces gráficas y de scripting. El interfaz gráfico permite administrar eficaz y fácilmente cualquier cambio. El interfaz de scripting permite automatizar cambios múltiples.
- Mecanismos de confección de plantillas. Éstos permiten poner a punto las herramientas para un uso administrativo eficiente en una institución específica dada o para la operación del sistema en forma repetitiva.
- Gran flexibilidad de la configuración. La flexibilidad de las arquitecturas de los productos de los servidores subyacentes se ve en los interfaces para la administración. Esta flexibilidad es muy importante en situaciones complejas donde el uso de muchos productos hace que finalmente no se cumplan los requisitos fijados para implementar las políticas deseadas.
- Excelentes rasgos de seguridad. Los sistemas de administración y los servidores subyacentes, tienen un rango de seguridad y servicios de

administración de seguridad tales como anti-spamming, control antivirus, y autorización.

- Permite concretar una arquitectura escalable sin esfuerzo o requisitos adicionales.
- El sistema puede mantener varios paquetes de configuración y cambiar entre los mismos según lo requieran los operadores. Aunque en algunos casos los servicios tienen que ser reiniciados para asumir la nueva configuración.
- Los roles de usuarios se implementan con derechos a acceso configurables. Cada supervisor se registrará mediante cuenta y clave de acceso.
- Un grupo de usuarios pueden registrarse simultáneamente.

MConsole: Administrador de Mensajería Institucional

El Administrador de Mensajería Institucional (MConsole) permite la administración de servidores de mensajería. Este es un DUA (Agente Usuario de Directorio) especializado que actualiza la información relacionada con la configuración de los servidores de mensajería en el Directorio.

El MConsole proporciona tanto un interfaz gráfico, como de scripting con todas las funciones requeridas. El interfaz gráfico está diseñado para hacer más simples las tareas, usando asistentes y pantallas de acceso simples con valores por defecto, dando también acceso a una configuración más detallada donde sea necesario.

El MConsole proporciona un sofisticado mecanismo de plantillas que permite cambiar el comportamiento de las pantallas. Esto permite adaptar el interfaz para diferentes implementaciones del sistema, y para tener en cuenta variaciones y requerimientos locales.

También puede accederse a las funciones de administración a través del interfaz Tcl scripting, lo cual es muy importante para facilitar la configuración remota de sistemas, y para automatizar procesos repetitivos. Esta doble aproximación a las funciones administrativas es una de las características más importantes de este producto.

Cada mensaje puede ser compuesto con un Latest Delivery Time. Cuando se cumple ese tiempo, el mensaje no se envía y se genera un Non Delivery Report al originador.

También es factible definir los Timeouts que tiene el QMGR en el MConsole. Ingresando en MConsole, se selecciona el MTA que será configurado, luego la pestaña Delivery (o también Queue Manager) a fin de acceder a muchos timeouts que están explicados brevemente en el Help de esa página, y mucho más en detalle en el manual SWADM.

Estos dos mecanismos funcionan perfectamente para sistemas que cumplen con la norma X.400. Si se cumple el timeout, entonces el mensaje es rechazado.

El requerimiento de que el mensaje se entregue a un supervisor es incompatible con la normativa X.400 ya si bien es factible de ser incorporado, el mensaje será

entregado al supervisor y no se genera la falla de entrega para el usuario original (no se genera un NDR).

Es factible proceder como sigue:

Se establece un timeout amplio, para los mensajes en función de su prioridad configurándolo desde MConsole.

Si se excede el timeout, los mensajes rebotan para el originador

Antes de que los mensajes reboten, puede llegar a establecerse un mecanismo de indicación basado, que alerte a los supervisores de que hay mensajes por vencer.

Los operadores, alertados de la demora, antes de que el mensaje sea rechazado toman acción sobre el mensaje.

El Mconsole entre otras cosas permite ver el contenido de los mensajes, y también redireccionar (al mail box del supervisor) un mensaje que se encuentra en la cola.

Pantalla del Administrador MConsole

Administración de usuarios

La administración de usuarios que permite agregar, administrar y eliminar usuarios es una parte fundamental en la configuración del sistema de mensajería. Se muestra a continuación un ejemplo de pantalla para configuración de un usuario. En cada caso, se tiene flexibilidad para seleccionar el servidor / máquina en donde los mensajes son entregados y también los parámetros asociados.

Se proporciona total soporte al Sistema Común de Direccionamiento.

Listas de distribución

El M-Switch soporta el uso de listas de distribución, y la configuración de estas listas puede realizarse usando el MConsole/SODIUM que interacciona con M-Vault.

Mapa local de direcciones

Una funcionalidad importante del M-Switch es la posibilidad de realizar varios tipos de mapas de direcciones. Se soportan tres tipos diferentes:

Sinónimo. Un sinónimo es un valor alternativo para una casilla de correo. Una característica importante de los sinónimos es que al mismo tiempo que forman un juego de nombres alternativos, también permiten escribir los encabezados de los mensajes en un "formato canónico". Esta reescritura en un formato consistente facilita la comunicación y reduce la confusión.

Alias. Un alias es como un sinónimo, excepto que sólo controla la entrega y no la reescritura. Un alias podría usarse para definir "web master" como un usuario específico.

Redirección. Una redirección es como un alias, sólo que cuando es procesado se graba como un redireccionamiento y, si se usa X.400, apunta a los elementos de protocolos apropiados. Esto es apropiado cuando se registra a un usuario del espacio de nombres local a un espacio de nombres fuera de la institución.

Esta flexible capacidad de “mapeado” es muy útil en grandes organizaciones o en instalaciones complejas.

Configuración del Message Switch

Para establecer una configuración inicial, existe la necesidad de colocar una cierta cantidad de información en el Directorio (llamada información básica o de núcleo) y apuntar los procesos del servidor hacia esta información.

Para facilitar esto, Mconsole/Switch Configuration contiene asistentes simples que ayudan en la preparación inicial. En la primera fase, la instalación permite sólo la selección entre " Mail de Internet solamente", "X.400 solamente", o "Ambos". Esta separación permite que los sitios que no usan X.400, no tengan necesidad de intercambiar datos relacionados con los sistemas X.400.

Se puede acceder de dos formas a la configuración del Directorio desde los servidores de mensajería:

- Poniendo en la ruta y, según las necesidades, información relacionada como la que se busca en el Directorio. Esto usa en el CLDAP optimizado (Protocolo Simple de Acceso a Directorio sin conexión: RFC 1798) ó X.500 DAP.
- O para que la información de la configuración del núcleo sea estable, utilizar un texto “a medida” que se genera desde el Directorio, con lo cual se optimiza el rendimiento.

La pantalla a continuación enseña el inicio del asistente para la incorporación de un nuevo MTA.

Árboles de Rutas

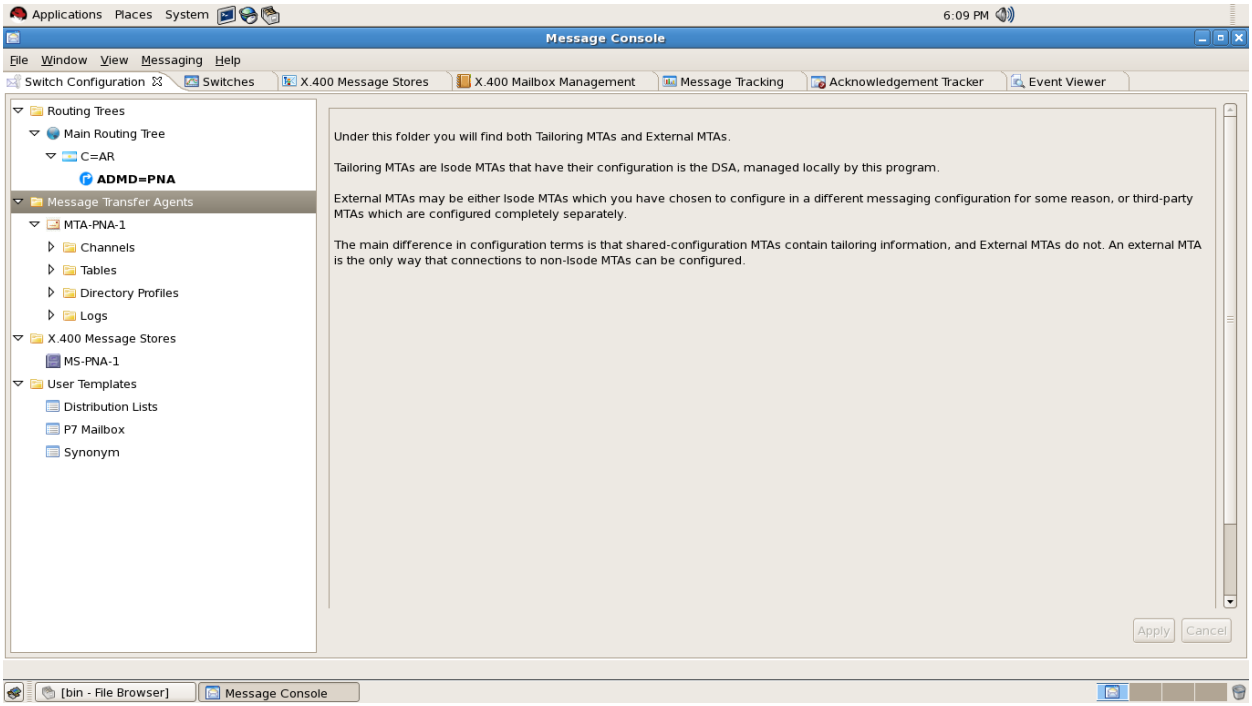
El concepto de “Árbol de ruta” es fundamental para los trabajos de administración de la configuración. Fue desarrollado para dar soporte al enrutamiento X.400 y esta técnica ha sido ampliamente adoptada por las empresas vendedoras de X.400.

El árbol de ruta permite la asignación de la información de ruta (incluyendo la de entrega a los usuarios) y que esto sea representado en un sub-árbol, o rama del Directorio. Un árbol de rutas se comparte en una comunidad de servidores. Esta “comunidad basada en el enrutamiento” permite compartir la información de una manera que optimiza el trabajo de configuración en una organización, y no expone información privada fuera de la comunidad.

El poder de esta característica es un beneficio muy importante que brindan las herramientas de administración que serán provistas.

Asignación de ruta X.400

El sistema soporta la configuración de rutas en X.400. Este servicio es muy flexible y permite el control eficaz del enrutamiento dentro de una organización, permitiendo además la configuración directa de conexiones bilaterales a ADMD X.400 y enlaces a PRMD.



El sistema también provee extensiones habilitando la integración para el Almacén de Mensajes (MS) P3/P7.

Configuración de troncales (Backbone)

Una configuración de esta naturaleza tiene muchas ventajas, pero aún así no es práctica para muchas organizaciones. En un Sistema de Mensajería Electrónica Segura SKS X400 será necesario dar soporte a distintos grupos de usuarios organizados en grupos de trabajo, y luego integrar a éstos con una troncal o “backbone”.

En configuraciones de grandes implementaciones donde se da soporte a usuarios locales utilizando Microsoft Exchange y sistemas heredados (legacy systems), el uso de la troncal provista ha demostrado ser muy eficaz. Esta sección y las siguientes, describen las capacidades de administración que convierten a los productos en una opción ideal para este estilo de configuraciones.

Esta configuración permite que partes de la organización sean limpiamente conectadas a la troncal, ya sea usando SMTP (el Mail de Internet) ó X.400. La forma más clara de manejar esto es delegar parte del espacio de nombres a una parte de

la empresa que está siendo conectada, (por ejemplo “@enterprise.com” delegates “@deptx.enterprise.com”). La troncal o backbone puede usarse para interconectar partes autónomas de la organización y proporcionar una conectividad completa.

El uso del canal del M-Switch permite luego enlazar a las partes diferentes de la organización para agruparlas según sus características, esto dará a menudo una importante flexibilidad en una configuración compleja

Administración Operacional del M-Switch

La administración operacional es el monitoreo y control del M-Switch que está basada en tres componentes visibles:

MConsole: consola gráfica que habilita el monitoreo y control de una o más copias del M-Switch.

Supervisión sin usar SNMP (Protocolo de Administración de Red Simple), en este caso el MADMAN (Administración de Correo y Directorio) y el MIBs (Base de Información Administrativa).

- Visor de registros archivados, usando el Visor de registros (Log Viewer).

Adicionalmente, puede optarse por realizar el monitoreo usando SNMP en base a cualquier monitor estándar de SNMP.

Todo el acceso a la administración operacional estará protegido a través de permisos y autorizaciones protegidos por contraseña.

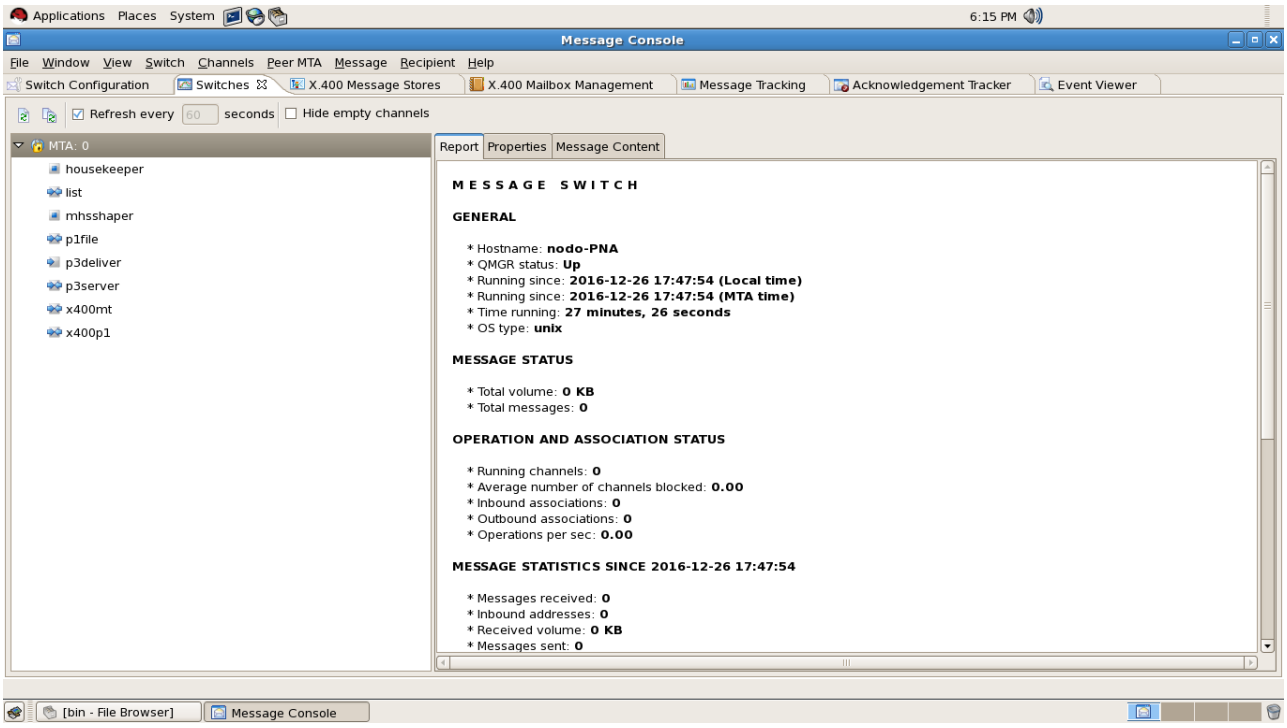
Los distintos módulos pueden invocarse transparentemente desde las posiciones de supervisión múltiples e intercambiables, que permiten que la supervisión del sistema cuente como mínimo con las siguientes funciones:

- Configuración del MTA Nombre, Unidad Organizativa, Organización, PRMD, ADMD, País.
- Configuración de usuarios locales Visualización, Creación, Edición, Borrado.
- Configuración de MTAs adyacentes Visualización, Creación, Edición, Borrado, de MTAs adyacentes.
- Configuración de Rutas Visualización, Creación, Edición, Borrado de las plantillas de ruteo.
- Monitoreo de la performance del sistema.
- Estadísticas del MTA.
- Estadísticas de un usuario.
- Visualización y monitoreo de mensajes en cola.
- Monitoreo de la operación del sistema.
- Trazabilidad de mensajes y visualización de eventos en el LogViewer.

- Alarmas (errores de autenticación de usuarios o MTA, detección de lazos de ruteo, abortos, etc.).
- Niveles de traceo y alarmas (niveles no deseados de cola de mensajes, estadísticas por usuario, etc.).
- Monitoreo de consumo de Recursos (utilización de facilidades, espacio en disco usado / disponible, capacidad de procesamiento usado, etc.).
- Shutdown/Restart del MTA.

Monitoreo del M-Switch y su módulo de control: MConsole

El M-Switch tiene una herramienta llamada MConsole, ilustrada debajo. La misma proporciona monitoreo y funciones de control para un M-Switch a nivel individual posibilitando las funciones descriptas en el párrafo anterior. MConsole proporciona un despliegue gráfico que muestra la historia de carga del M-Switch y proporciona el estado de varios "canales" por los cuales el mensaje ha sido enrutado, mientras que resalta cualquier problema en la cola de mensajes o en los mensajes. Tiene una sofisticada tecnología heurística configurable para clasificar múltiples niveles de advertencia. También permite el control de la cola de mensajes, y posee capacidades como la de reenvío y eliminación de mensajes.



Hay una versión de línea de comando de MConsole (el LConsole), que puede utilizarse para integrarse en otras aplicaciones.

Las colas de transmisión son manejadas a través de la Consola de Supervisión (GUI) del accediendo el supervisor a la facilidad de monitorear y supervisar en tiempo real la cola de mensajes de salida. Para el caso en que se desee tratar selectivamente uno o más mensajes de esta cola, el supervisor no tendrá más que seleccionar y mover el mensaje a la posición de supervisión y luego allí realizar la tarea deseada o bien reencolar el o los mensajes movidos.

La cola de transmisión es ordenada por prioridad y dentro de ese orden por fecha de entrada en cola, no posee un tope ni restricción de ningún tipo en cuanto a cantidad de mensajes pues estos deben permanecer en cola, hasta tanto sean transmitidos según parámetros de cada canal en particular y según la performance del vínculo de comunicación para lo cual estará involucrado el otro extremo de la línea y los recursos que el sistema de transporte y recepción remoto soporte.

El redireccionamiento de mensajes hacia otro MTA se encuentra establecido dentro de las políticas de seguridad. A fin de garantizar la seguridad operacional, a nivel del MTA/MS no existe posibilidad de borrar mensajes ni generar inconsistencias.

Monitoreo general del sistema

A nivel del MTA

M-Switch soporta el monitoreo con SNMP (Protocolo de Administración de Red Simple) y el MADMAN (Administración de Correo y Directorio) MIBs (Base de Información Administrativa) y MADMAN. Esta última aplicación incluida en el conjunto de aplicaciones que componen el MTA, define los mecanismos para supervisar el estado de un M-Switch, mientras entrega información que incluye el estado general, el número de mensajes en las colas, etc.

Esta funcionalidad permite supervisar un sistema integrado por un gran número de M-Switches al mismo tiempo. Este monitoreo integrado es una característica muy deseable para grandes instalaciones que proporcionen servicios 24x7. Esto también permite que el sistema que supervisa pueda ser compartido fácilmente e integrado con otras funciones.

Para permitir la supervisión de la Terminal, la interfaz gráfica tiene un registro especial donde la mayoría de los eventos relevantes es anotado, por ejemplo: el inicio y el apagado de una máquina, la entrada y salida de un usuario, la realización de copias de respaldo, la restauración de archivos, el cambio de interfaz de comunicaciones, los cambios de configuración, los cambios de fecha y hora, etc.

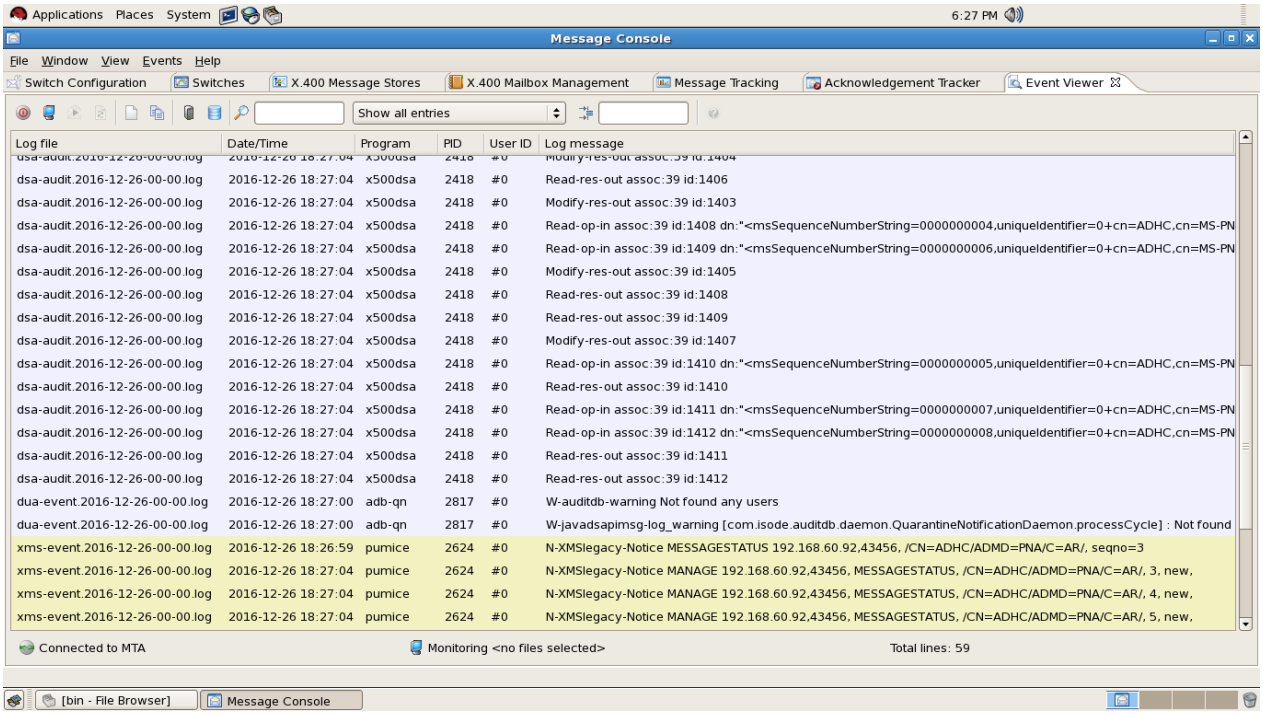
A nivel del MTA/MS, el monitoreo se obtiene a través del MConsole y el diagnóstico y supervisión de los recursos del sistema gracias a la aplicación de supervisión del SNMP.

Los eventos principales del sistema se complementan con el registro para la actividad de los Agentes Usuarios, lo cual integrado con la administración y monitoreo remota permiten el CONTROL TOTAL DEL SISTEMA.

Los archivos y registros llamados “logs del sistema” permanecen disponibles hasta su depuración manual y periódica. Si bien comprenden una gran cantidad de

información tipo texto, no generan archivos voluminosos que comprometan la capacidad de almacenaje, pudiéndose almacenar dos o tres meses sin afectar el servicio. Luego pueden respaldarse sobre cinta.

A continuación se presenta una pantalla de eventos del LogView aplicación que ha sido llamada Rufus.



Administración Remota

M-Switch también cuenta con una herramienta de registro (log) configurable. Esta herramienta trabaja sobre protocolos accesibles remotamente, y así puede realizarse la tarea de seguimiento del registro en forma remota. La herramienta puede usarse para manejar múltiples servidores y archivos de registro, y viene con una gama de posibilidades de seguimiento y administración.

En forma similar, la Terminal puede operarse y controlarse remotamente, un rasgo que ha demostrado ser inestimable cuando se opera en soporte de sitios remotos.

A un requerimiento del administrador, el operador ve un aviso en el cual se requiere su autorización para que su Terminal pueda ser administrada remotamente. Una vez aceptado, el administrador remoto puede arreglar o configurar la Terminal como si estuviese en el lugar.

El interfaz gráfico de la Terminal tiene un registro especial donde la mayoría de los eventos relevantes es anotado, por ejemplo: el inicio y el apagado de una máquina, la entrada y salida de un usuario, la realización de copias de respaldo, la restauración de archivos, el cambio de interfaz de comunicaciones, los cambios de configuración, los cambios de fecha y hora, etc.

CONSOLAS DE SUPERVISIÓN

La cantidad de consolas usadas para monitorear el sistema puede ser modificada a requerimiento de la administración. Todas las aplicaciones de monitoreo y supervisión pueden ser presentadas en pantallas múltiples en una sola consola o en diferentes configuraciones de la consola. Esta configuración puede modificarse en línea sin interrupción de la operación usando teclas configurables o por medio de comandos simples. La falla de una Terminal no afectará el rendimiento de las restantes.

Nuestra experiencia sugiere, para un sistema del tamaño medio, el uso de posiciones de supervisión, cada uno enlazado con una consola doble.

Respecto de las consolas, proveeremos dos (2) solicitadas, si bien recomendamos la siguiente distribución:

- Posición de supervisión del MTA.
- Posición de supervisión del MS y supervisión de la red integrada (una consola para cada utilidad).
- Opcional: una posición con dos consolas adicionales para estadísticas y/o vistas de Administración / Monitoreo.

Sistema de alarma incluyendo las advertencias visuales y sonoras

Estos servicios son normales en nuestros sistemas y pueden configurarse a gusto del cliente.

Se asignan los eventos de sistema a tres categorías:

- las alarmas
- las alertas (dependiendo de la severidad)
- información de Estado del Sistema.

Respecto del Tráfico: Estas alarmas ocurren tanto a nivel del supervisor como del operador. La Terminal proporciona indicaciones de alerta al usuario humano siempre que se reciba un mensaje.

A nivel del MTA y de todos los eventos relativos al tráfico y aquéllos generados automáticamente llegan a la Consola de Servicio y ésta proporciona las alarmas que se hayan configurado. Alarmas operacionales: Están relacionadas con el estado de la red, el estado de los subsistemas, los recursos del sistema, el estado de la cola de transmisión, el contenido de cola de transmisión (la cantidad de mensajes en la cola, secuencia pendiente de transmisión según creador y prioridad, identificación del mensaje más antiguo en la cola, etc.).

Se generan específicamente por:

- Mconsole para MTA y MS
- por el agente de SNMP

Todos estos eventos se notifican a la consola de supervisión.

Es posible activar una secuencia de comandos (script) asociado con ciertos eventos para activar una alarma externa de sistema (acústica, óptica, etc.).

Es posible asignar los eventos a una impresora de eventos para obtener una copia impresa automática del evento.

Seguridad y control de acceso

Hay muchos aspectos sofisticados que se relacionan con la seguridad en el sistema, pero es notable el hecho de que el paquete de programas de la Terminal puede tomar el control del sistema operativo, bloqueando los comandos de acceso al OS, e impidiendo el mal uso o el abuso en la utilización de la Terminal. A continuación se describen otras características:

Características de administración de la seguridad del sistema de mensajería.

El sistema de mensajería tiene un amplio control sobre la seguridad. El sistema de autorizaciones se describe en las secciones siguientes.

El sistema mantiene el soporte a la seguridad que de por sí ya ofrece el X.400, incluso el control de la contraseña de todas las asociaciones. Esta funcionalidad puede manejarse desde el MConsole. Para la autenticación estricta es necesario establecer también una autoridad de certificación.

Seguridad del sistema administrativo

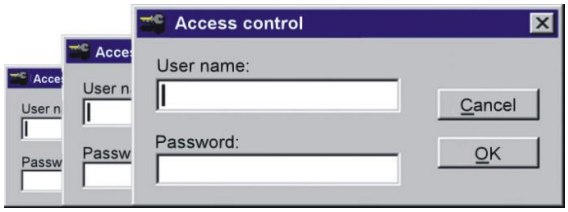
La administración del sistema en sí misma contiene también cuestiones relativas a la seguridad y es importante considerar:

- Si es la aplicación MConsole quien se conecta al Directorio, se usa X.500 DAP. Una de las razones para esta opción es que DAP soporta la autenticación estricta y es actualmente el único protocolo de Directorio abierto que permite hacer esto.
- Si en cambio los servidores de mensajería se conectan al Directorio. Los servidores de mensajería normalmente acceden el Directorio con CLDAP, que no soporta previsiones de autenticación. En este caso recomendamos que el servidor que accede con CLDAP corra en la misma máquina que el servidor de Directorio y así, la configuración de la asignación de rutas se fija sólo para restringir el acceso desde la máquina local (brindando así la seguridad requerida).

Autorización

Para la Terminal:

Para lograr una correcta administración, el sistema permite establecer 3 niveles/roles de usuario con diferentes claves. Estos podrán registrarse simultáneamente.



La computadora utilizada puede también ser restringida para uso exclusivo como Terminal. En este caso, la aplicación asume el control inmediato del sistema operativo desde el inicio del sistema y no permite acceso a cargar o modificar programas.

A nivel de MTA:

El sistema ofrece un sofisticado paquete de autorización de mensajes, para permitir el control del flujo de mensajes. La autorización tiene varios aspectos.

- La política. El núcleo de la configuración está modelado en base a varios canales, organizando los usuarios y sistemas mensajería agrupados por canal. Esta agrupación puede organizarse de una manera muy general, y sirva además como una base para la aplicación de políticas flexibles. Las políticas de administración básicas pueden formar rutas entre canales “libres”, “bloqueados” o sujetos a una posterior autorización.
- Control de usuario. Concede o niega el acceso a los usuarios de correo conocidos.
- Control del M-Switch. Esto concede o niega el acceso a conmutadores de mensajes (M-Switches) específicos (y a determinadas rutas).
- Control de contenido. Ambos controles anteriores pueden modificarse según el tamaño o el contenido del mensaje (por ejemplo, para prevenir el envío de mensajes de gran tamaño en algunas situaciones o cuando el ancho de banda es insuficiente).
- Advertencia. Hay varias opciones para establecer advertencias y notificaciones de violaciones.
- Estos controles pueden usarse para preparar varios tipos de controles. Por ejemplo:
- Ciertas listas de distribución no pueden tener acceso permitido para usuarios externos.
- El usuario A puede hacer envíos al usuario B que está relacionado con un usuario, pero no al C que está relacionado con el mismo usuario anterior.

TERMINAL AGENTE USUARIO

La Terminal fue creada originalmente por nuestros ingenieros, que utiliza modernas herramientas de software y comunicaciones.

Siguiendo el estado de la técnica de las comunicaciones ha evolucionado y funciona con el nuevo concepto Sistema de Mensajería Electrónica Segura SKS X400 para las redes LAN/WAN, utilizando protocolos X.400 P3 ó P7 para comunicarse con el MTA/MS, asumiendo las funciones reales de un Agente Usuario (UA) y a través de DAP (los protocolos X500) se comunica con un DS, funcionando como un Agente Usuario de Directorio (DUA).

La Terminal tiene múltiples posibilidades de conectividad. Puede intercambiar información a través de diferentes vínculos físicos como líneas punto a punto o redes punto a multipunto, y también soportar diversos tipos de dispositivo tales como:

- Puerto serie Asincrónico (RS232)
- Convertidores EIA to loop
- Micro-módems de audio
- Placas de red Ethernet (alámbricas o inalámbricas)

La Terminal soporta los alfabetos IA5 e ITA2, y X.400 y las normas X.500 / LDAP ITU-T.

Recepción y auto validación

Cuando se recibe un mensaje de correo, el software detecta automáticamente el tipo de mensaje, el formato, el número de serie y toda la información relacionada con el mismo, mientras comienza el proceso de comprobación de validez.

Proceso de Impresión

La Terminal puede ser configurada para imprimir en forma manual o automática. Si se selecciona la impresión manual, el mensaje se retiene en la cola de entrada para que sea visto por los operadores. Si se detecta un error, el operador recibe una alarma visual o sonora y se genera un mensaje de servicio que es transmitido al supervisor y al emisor del mensaje. Todos estos procesos son automáticos

Fácil transferencia y almacenamiento de datos o mensajes

El almacenamiento o transferencia de mensajes utilizando dispositivos externos es realizado de manera muy fácil y permite codificación previa, facilitando de este modo la actualización o el mantenimiento de las terminales. Trabajando dentro de un ambiente del Sistema de Mensajería Electrónica Segura SKS X400 el mensaje

puede tener partes adicionales en su cuerpo (adjuntos) para que diferentes tipos de archivos como imágenes, hojas de cálculo y otros, puedan ser transferidos entre estaciones de la red. Estas partes de mensajes también pueden codificarse.

Los mensajes permanecen disponibles en el LMS (Local Message Store) que posee cada Terminal por el tiempo que se le defina en el correspondiente parámetro, de manera que los mensajes permanecen para ser consultados y/o recuperados para su reprocesamiento, para ello el operador cuenta con una herramienta de búsqueda de mensajes en donde puede entrar los distintos datos y rangos de búsqueda que permita el filtrado de los mensajes, asimismo el Terminal cuenta también con la posibilidad de realizar periódicamente sendas copias de respaldo que podrán ser permanentes dentro del disco rígido de la Terminal o volátiles entrando en un ciclo en el que cada backup es sobrescrito con el siguiente luego de la décima copia respaldo, en otras palabras este ciclo permite contar permanentemente con las últimas 10 copias de respaldo. También es posible salvar copias de mensajes en medios removibles.

Además de estas herramientas, la Terminal posee también la facilidad de poder recuperar mensajes de entrada desde el servidor accediendo al almacenamiento de corto plazo del MS mediante un formulario de consulta que posee la GUI.

Para el supuesto caso en que el mensaje se encuentre dentro del almacenamiento de largo plazo y por alguna circunstancia el operador no pueda encontrarlo en la Terminal ni en los backups de ésta, podrá solicitar el mensaje al supervisor del sistema quien deberá reinsertar el mensaje nuevamente en el mail box (casilla) del usuario correspondiente mediante la consola del MS.

Los mensajes pueden tener el destinatario primario, un destinatario de copia y también el destinatario de copia invisible (u oculto).

Es posible también especificar el tiempo de validez de un mensaje. Dentro de los objetos de información que posee cada mensaje del mundo X.400 existe una variable denominada X400_S_LATEST_DELIVERY_TIME que permite asignar el tiempo de vencimiento el cual se mide de extremo a extremo. El Terminal ofrecido cuenta con la posibilidad de configurar esta opción para cada mensaje y el sistema asignar el tratamiento correspondiente para el caso en que un mensaje sobrepase el vencimiento, emitiendo automáticamente los correspondientes reportes).

Servicio continuo

Durante cualquiera de los procesos recién descriptos la Terminal mantiene su capacidad de recepción o transmisión de mensajes. Ante el caso de falla de una Terminal, independiente del problema, dicho suceso no afectará el normal funcionamiento de las demás terminales.

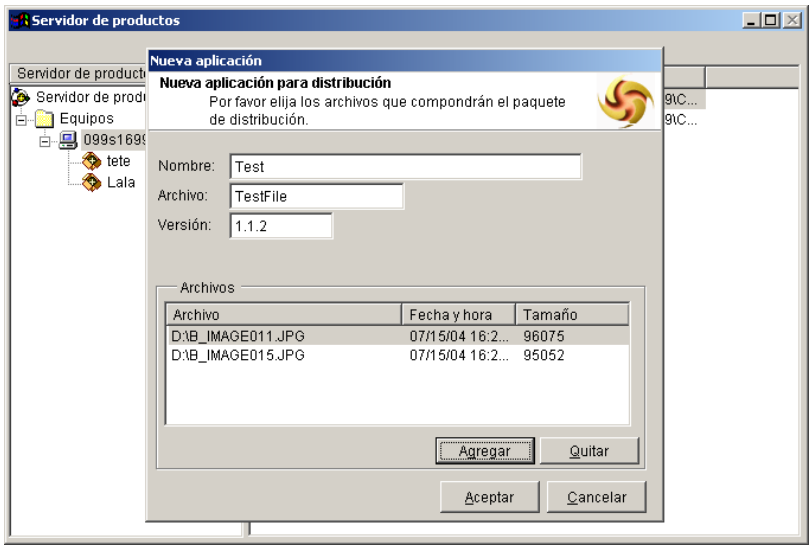
Actualización remota automática

Existen dos tipos de actualización automática de las Terminales:

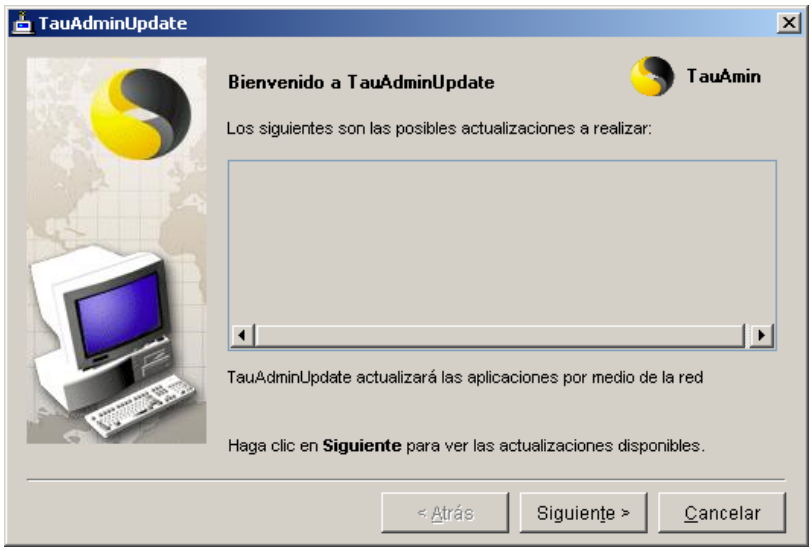
- Actualización de bases de datos.
- Actualización del paquete de programas

Actualización del paquete de programas

Después de un reinicio de la Terminal, cada subsistema verifica las versiones del software contra el servidor de software / configuraciones. Si una o más versiones nuevas están disponibles en el servidor de actualización, las terminales solicitan la nueva versión y la instalan automáticamente. Después que una Terminal se ha actualizado, envía un mensaje al servidor, el cual guarda el registro de que la misma se ha puesto al día. Estos servidores fueron denominados Terminal de Usuario AdminServer. A continuación mostraremos algunas pantallas:



En la Terminal, el usuario verá el Terminal de Usuario AdminUpdate como se ve abajo:



Funcionalidades

Todos los menús y avisos para esta oferta están en español. En orden a reducir el trabajo del operador, reforzar la seguridad del sistema y su disponibilidad, Terminal de Usuario tiene diversos procesos automáticos para recuperar mensajes perdidos en caso de que falle el sistema.

El operador puede:

- Elegir opciones relativas a mensajes como: informe de entrega, recepción, prioridad e importancia.
- Acceder a las funcionalidades de Terminal de Usuario mediante el uso de mouse o teclado (también posee métodos de teclado abreviados).

Para la recepción del mensaje hay muchas opciones posibles, entre ellas el envío de los mismos a una lista de direcciones predefinida (ya sea un Macro o una Lista de Distribución) aplicando criterios de filtrado como: Prioridad, Originador y Categoría del mensaje.

- Al originar mensajes, el usuario puede pedir:
    1. un informe de entrega del mismo
    2. un informe de recepción (si el mensaje es de alta prioridad, el informe será generado automáticamente por el recipiente)
    3. establecer prioridades
- Conseguir información adicional sobre mensajes transmitidos como
    1. el estado de la transmisión,
- Clasificarlos según:
    1. el tamaño,
    2. fecha y hora de transmisión,

3. fecha y hora de su lectura.

- Un informe de entrega y notificación para cada destinatario

La Terminal puede asignarse a más de una dirección, expandiendo las posibilidades de cada sitio para soportar varios operadores.

Se proporciona también la función de creación de carpetas de mensajes y la personalización de su uso.

La Terminal tiene un completo sistema de ayuda en línea, de fácil acceso para los operadores, y que proporciona un enlace automático a la explicación de funciones y características con un estilo de simulación de funcionamiento que permite al operador ver las consecuencias de una acción. El sistema de ayuda se complementa con un sistema de operación remoto que permite a los supervisores tomar el control de una Terminal y ayudar a distancia al operador respecto de las funciones que necesita entender y realizar.

Esta funcionalidad también se usa para la configuración remota de una Terminal, eliminando la necesidad de presencia en sitio por parte del supervisor.

Pantallas disponibles

Se dispondrá de pantallas de presentación para la generación / recepción de mensajes y además, posee otras pantallas y funcionalidades como:

- Informe en pantalla de mensajes en cola de espera.
- Informe en pantalla de mensajes recibidos.
- Informe en pantalla de mensajes transmitidos.
- Confirmación de la entrega: para cada mensaje transmitido.
- Registro histórico de los eventos en la Terminal.
- Ayuda.
- Campos de formularios en pantalla bien descriptos y complementados por una barra de estado y menús desplegables.
- Generación del mensaje, incluyendo pre-formatos y plantillas.

El HMI se desarrolla como un interfaz gráfico (GUI) fácil de usar, de respuesta inmediata a la presentación de datos. Tiene menús automáticos, desplegables, y ayuda en línea y en pantalla.

Redactar un mensaje es un proceso fácil realizable por selección de plantillas incorporadas que ayudan en el ingreso de datos y controlan su validez. Los mensajes no pueden enviarse si no cumplen con los requerimientos de validación.

El programa controla estrictamente el ingreso de datos mostrando cambios de color en los campos validados y bloqueando la posibilidad de envío del mensaje si los datos mínimos necesarios no son correctos.

La validación ocurre a nivel de carácter y longitud de campo así como a nivel lógico y tiene como referencia una base de datos interna que contiene los datos.

Formularios y plantillas incluidos en Terminales de Usuario

Todas las Terminales pueden presentar plantillas y formularios en idioma Español, se podrá validar datos para facilitar el trabajo de los operadores y de la función de supervisión al lograr que las terminales no envíen mensajes incorrectos.

Antes de la transmisión, todos los datos se convierten al formato seleccionado y son empaquetados para luego colocar el mensaje en la cola de salida donde se agrega el número de serie. Todos estos procedimientos son transparentes y son automáticos para el operador.

Los mensajes, así preparados en sus formatos, quedan disponibles para su visualización, transmisión, grabado, pueden quedar pendientes, ser cancelados o inmediatamente impresos.

Se podrá solicitar la incorporación de nuevos formularios. Con respecto a los detalles de cada formulario, los campos de completamiento obligatorios (indicados debajo) se remarcarán en color amarillo, permaneciendo en esa condición hasta que el operador llene el campo de caracteres que completen el contenido sintáctico o semántico requerido, o hasta que se valida el contenido. Si así no fuese, el color del campo permanece inalterado y la Terminal no permite enviar el mensaje.

Una vez que se completan los campos obligatorios se presentan las siguientes opciones:

- Si se elige enviar el mensaje, la pantalla muestra un aviso diciendo que el mensaje ha entrado en la cola de la transmisión para ser enviado.
- Si se decide guardar el mensaje sin enviarlo, la pantalla confirma el guardado, al tiempo que indica cómo recuperar el mensaje si más tarde se decide enviarlo.
- Si se decide visualizar el mensaje, la pantalla muestra una presentación general del mensaje, permitiéndole al operador descubrir los errores.

Sistema de Validación

Para habilitar la validación en el ingreso de datos, el sistema tiene bases de datos estáticas ubicadas en cada Terminal. Estas bases de datos se actualizan automáticamente por medio del software llamado Subsistema Automático de Actualización de Datos, compuesto por una base de datos general instalado en un servidor que permite que una de las terminales de supervisión introduzca las modificaciones dictadas por la Autoridad correspondiente. En cuanto la actualización es ingresada, este servidor envía los mensajes con texto codificado en un formato definido para cada transacción de modificación de bases de datos hacia todas las terminales remotas.

En el servidor, una tabla registra las terminales que reconocieron la actualización y respondieron una vez que tuvieron actualizada su base de datos interna.

Las terminales tienen el software que les permite reconocer la transacción insertada en el texto codificado, iniciar la decodificación respectiva, y actualizar la base de datos respectiva automáticamente.

Transacciones disponibles:

Las siguientes transacciones están disponibles:

- Entrada de registro
- Corrección de registro
- Invalidación de registro

Descripción Técnica de la Terminal:

A continuación se hace una descripción técnica de los principales aspectos a considerar:

- Aplicación multitarea de 64-bits (trabaja tanto en primero como en segundo plano), desarrollada usando distintas herramientas bajo sistema operativo Windows 10 o superior.
- Procesamiento en tiempo real.
- Compatibilidad con protocolos de redes LAN / WAN sobre TCP / IP, y posibilidades de vinculación con otros sistemas de mensajería electrónica.
- Compatibilidad con protocolos STANAG 4406, X.400 y X.500/LDAP (y otros tipos de red a pedido).
- Validación de semántica, sintáctica y lógica de datos usando formularios y plantillas.
- Configuración personalizable.
- Administración de usuarios y del sistema por asignación de privilegios.
- Supervisión y monitoreo remotas.
- Plataforma multiusuario.
- Total cumplimiento con las recomendaciones y estándares del ITU-T y OTAN.
- Múltiple capacidad de conexionado por medio de una gama amplia de dispositivos, incluyendo la posibilidad de acceso LAN Ethernet duplicado.
- Métodos de cifrado y descifrado personalizados por el supervisor de la red.
- Interfaz gráfica del usuario (GUI).
- Mínimos requisitos de hardware.

- Capacidad de almacenamiento a largo plazo de todos los mensajes y sondas recibidos para un período de por lo menos 30 días. Se genera un registro diario también bajo un archivo único cuyo nombre contiene información de la fecha.

Almacenamiento:

Los tiempos de búsqueda de mensajes en el almacenamiento de corto plazo siempre serán menores a los tiempos de búsqueda en el de largo plazo en tanto que dicho plazo es directamente proporcional al volumen de la información en la cual se realiza la búsqueda.

Los mensajes en el almacenamiento de corto plazo (ACP) permanecen en cada casilla de correo (mail box) de cada usuario y pasan al almacenamiento de largo plazo (ALP) en forma totalmente automática mediante el proceso de resguardo. Todos los días a la hora de menor tráfico, generalmente en la madrugada, el proceso de resguardo y depuración se ejecuta como servicio configurable comprimiendo y copiando los mensajes que pasan así al ALP. Allí permanecen disponibles en el File System durante el tiempo que se desee parametrizar permitiendo la rápida reinserción de cualquiera de los mensajes.

El tercer nivel de almacenamiento es el del back up en cinta.

Archivo y recuperación de mensajes para propósitos legales u operacionales: Todos los mensajes pueden guardarse hasta un año a partir de una fecha indicada. El operador o supervisor puede investigar mensajes usando campos que filtran la búsqueda, por ejemplo, por tipo del mensaje, fecha de envío o recepción, rango números de serie, texto incluido, etc. El proceso de limpieza puede programarse para anular automáticamente todos los mensajes con un año de antigüedad. Hay además otras opciones disponibles.

Copias de respaldo:

Este proceso puede hacerse a pedido, a nivel de la Terminal. Puede guardar hasta diez copias de seguridad. La undécima copia de respaldo anula a la copia de respaldo más antigua. En caso de una falla, el sistema puede restaurarse usando cualquiera de las copias de respaldo realizadas.

A nivel de sistema, se configura mediante scripts que disparan distintas alternativas para realizar las copias de respaldo a un medio de cinta.

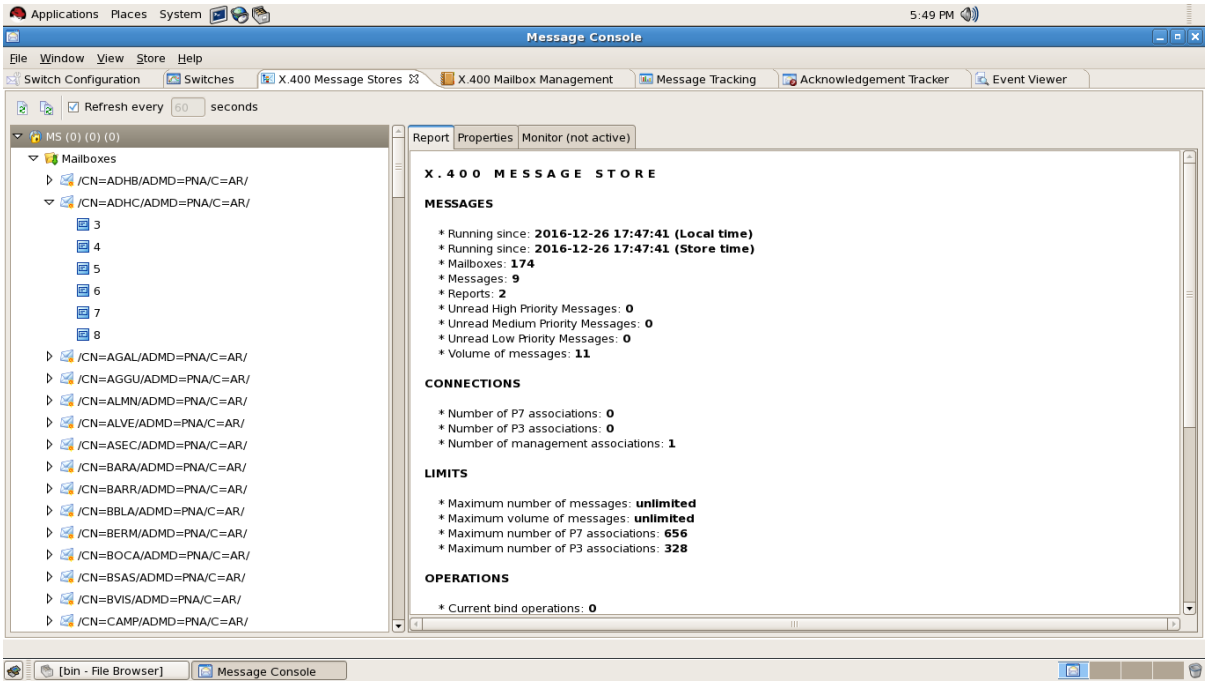
Registro y trazado de mensajes:

Se incluye un muy completo registro de actividad en los servidores que permite el seguimiento y el conteo de todos los mensajes, incluso el soporte para el registro de auditoria. El subsistema de registro posee capacidad total de localización de fallas y puesta a punto.

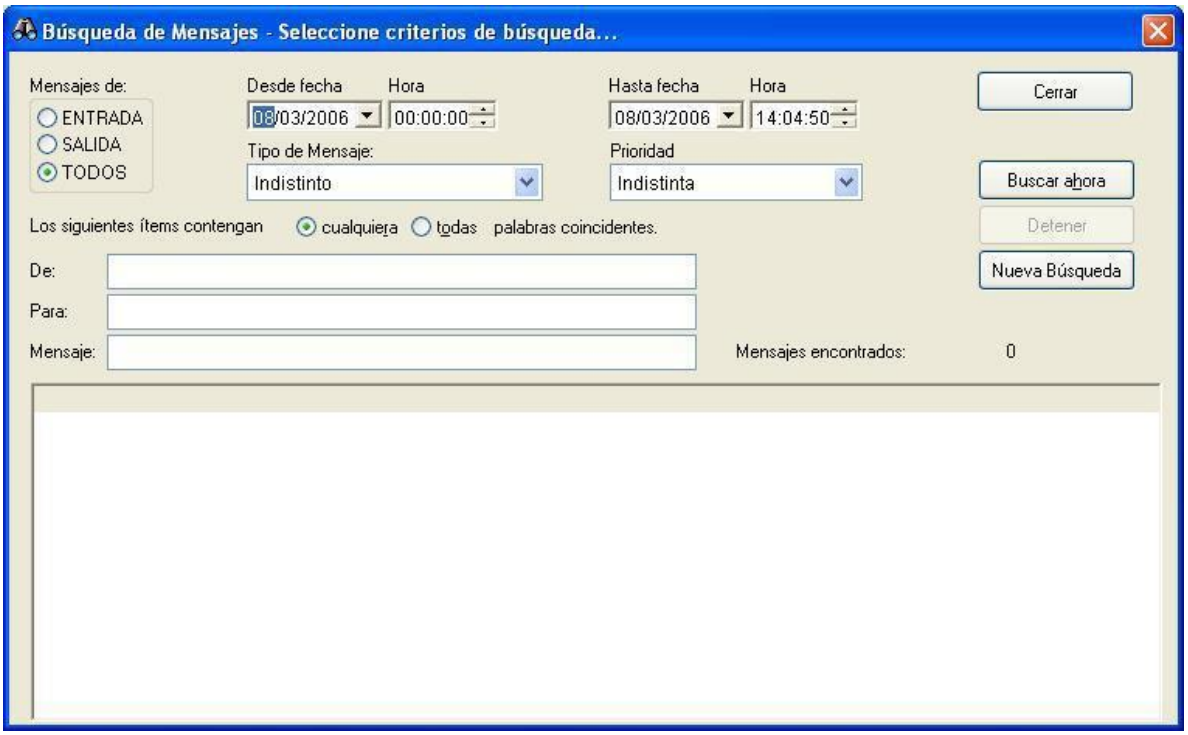
También es posible llevar registros a largo plazo de la información sobre mensajes enviados o recibidos por el MTA/MS. El registro está sólo limitado por el hardware disponible.

En orden a generar los registros diarios y para hacer copias de respaldo de los mensajes, el sistema realiza una operación configurable de copiado de respaldo hacia un dispositivo de cinta, al tiempo que genera un registro día por día, para luego realizar una “operación de ordenamiento” que no afecta a los mensajes no leídos.

El seguimiento de mensajes es realizado desde MConsole en la siguiente pantalla Servidor/Supervisor:



O desde la siguiente pantalla Agente Usuario/Operador:



OPCIONAL

CLIENTE MÓVIL SKS MAIL

SKS Mail es un cliente de correo para los dispositivos móviles disponibles en el mercado, que posee todas las funcionalidades y herramientas de un cliente de correo moderno.

Desde su concepción, el correo SMTP tiene sus raíces en el ámbito académico y su uso fue generalizado en un ambiente relativamente benigno y abierto por los cual su seguridad es limitada, pero la simplicidad y flexibilidad son su principales fortalezas.

Considerando estas concepciones y premisas, hoy por lejos es la aplicación más popular que comunica a través de Internet.

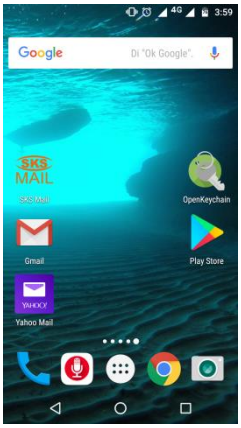
Hay que considerar que SMTP carece de auditorías y seguimiento confiables, lo que permite que un tercero se pueda hacer pasar por el originador de un mensaje o reenviar un mensaje en nombre de otra persona sin que la dirección original esté adjunta al mismo cuando éste llegue a su destinatario.

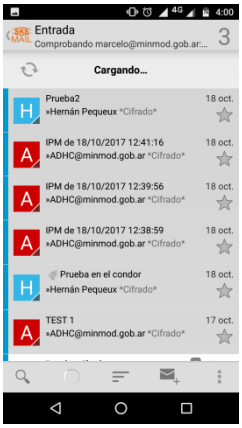
Skysoft Servicios S.A. ha desarrollado un cliente SMTP móvil (SKS Mail) que permite enviar y recibir mensajes desde y hacia la red segura X.400 utilizando conexiones seguras STARTLS sobre protocolos SMTP e IMAP, imposibilitando de esta manera que los mensajes sean intervenidos, aún si son enviados desde redes públicas.

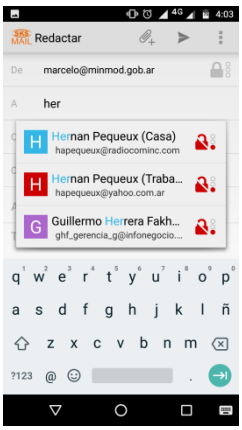
Este cliente de correo también cuenta con la posibilidad de enviar y recibir los mensajes cifrados, como así también los que no estén cifrados de la red X.400. A su vez, también cuenta con la capacidad de firmar o chequear la firma digital de los mensajes.

Otra de las características importantes de SKS Mail es que los mensajes cifrados se almacenan en el dispositivo conservando el cifrado propio, por lo que seguirán seguros aún si el dispositivo es extraviado.

La interfaz de usuario y su utilización ha sido simplificada para agilizar su operación.







Capturas de pantalla de SKS Mail

III. ESTRUCTURA DEL SISTEMA

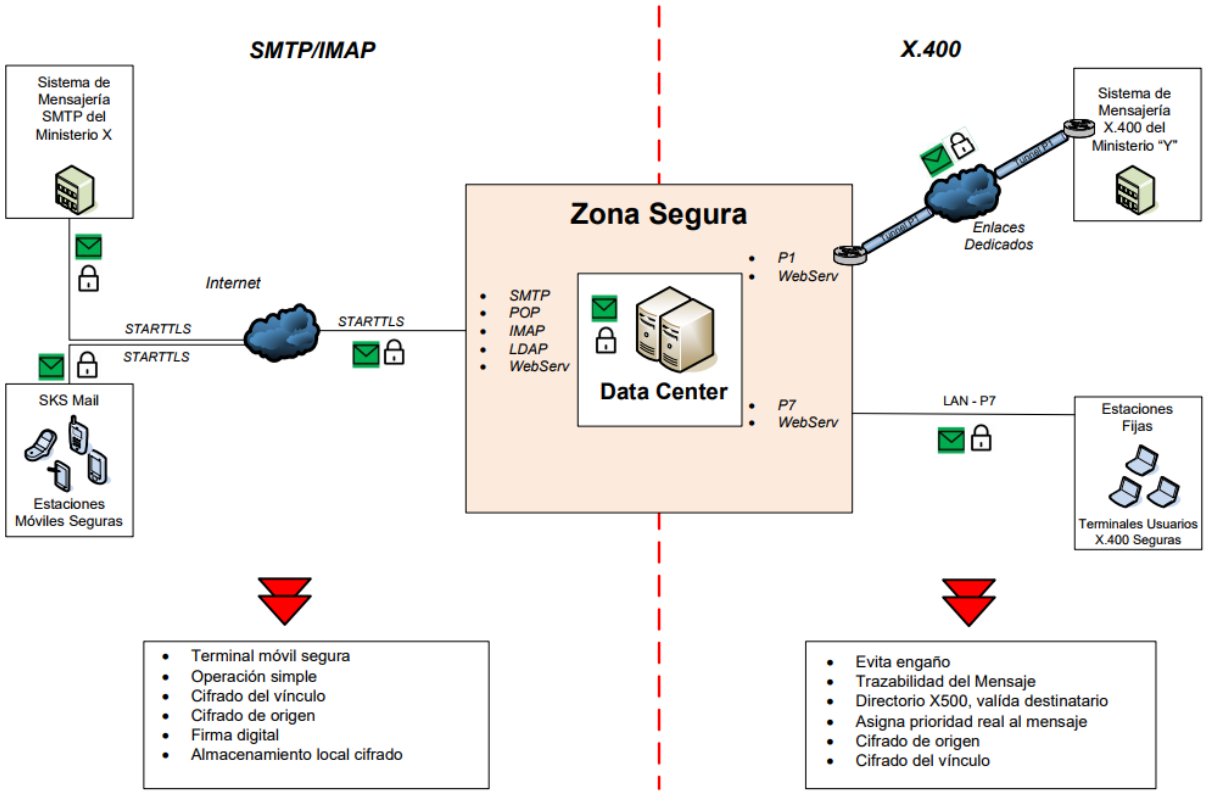
Arquitectura:

El sistema se integra en base a los siguientes servicios o aplicaciones que corren sobre uno ó más servidores y clientes según se dimensione el sistema.

- MSwitch MTA/MS (Servidor de Mensajería ATS X400)
- MVault DS (Servidores de Directorio X 500)
- Aplicaciones para Administración y Supervisión
- Terminal Agente Usuario

A su vez sobre el hardware de los servidores y/o clientes existe la posibilidad de implementar distintos sistemas operativos. Nuestros sistemas, normalmente están basados en los siguientes sistemas operativos: Windows 7 o superior para los Terminales, y Unix/Linux Red Hat Enterprise para los servidores principales del MTA/MS/DS.

A continuación se observa una representación "esquemática" de los componentes y estructura del sistema.



Conectividad

Para realizar la conectividad LAN se ha previsto que de acuerdo a la arquitectura recomendada por los principales proveedores de sistemas de networking, se instalará un sistema de conmutación integrado por un switch o router Cisco de acuerdo a las necesidades que surjan de los relevamientos.

Estos conmutadores han sido seleccionados para proveer una total administración y configuración remota desde la consola supervisora central. El sistema podrá utilizar opcionalmente la configuración propuesta de “WhatsUp Gold de Cisco Works”.

Software

La arquitectura del sistema es totalmente modular, basada en diversos servicios de aplicación.

Hemos hecho el esfuerzo de realizar nuestras soluciones tan independientes del proveedor del hardware como fuese posible así como también de los sistemas operativos, ya sea Windows o Linux/Unix.

El otro principio de construcción de nuestro sistema es su modularidad, permitiendo el reemplazo de hardware o de aplicaciones de software para actualizarlas siguiendo la evolución de la tecnología.

Este principio nos ha dado la ventaja de obtener una gran flexibilidad (también con respecto a las capas de transporte de OSI) lo que nos permite ofrecer soluciones para administraciones que tienen que cubrir una gran disparidad en su infraestructura de comunicación.

Todos nuestros sistemas se proporcionan con los discos de la instalación originales, las licencias perpetuas no exclusivas necesarias y no revocables, y los manuales de operación del sistema en idioma español.

El sistema está diseñado en base al modelo de arquitectura cliente-servidor y en el modelo de referencia de Interconexión de Sistemas Abiertos OSI.

Confiabilidad y Disponibilidad

Nuestros sistemas se proveen con servidores redundantes y periféricos y se configuran para ser conectados sobre la LAN existente.

Implementación del Proyecto, Instalación y Puesta en Marcha

Una vez adjudicado el sistema se determinará el diseño final, el que será aprobado por personal de la empresa/organismo.

Toda la instalación de los sistemas será realizada por personal de nuestra empresa con participación de personal de la empresa/organismo.

Se adjuntará un Cronograma donde se presentan las principales actividades para instalar y entregar operativamente el Sistema de Mensajería Electrónica Segura.

Durante la instalación se elaborará y proporcionará un registro de mantenimiento con todas las reparaciones, modificaciones, rediseños, alineaciones, fallas y actividades relacionadas con el sistema.

IV. Cumplimiento de los Protocolos X.400/X.500

El M-Switch X.400 provee amplio soporte para X.400, incluso para las versiones de la norma de 1984, 1988 y 1992.

El soporte central es para el Protocolo (P1) de Transferencia de Mensajes X.400, que es el protocolo usado para interconectar los Agentes de Transferencias de Mensajes X.400 (MTAs) y P3 y P7 que habilitan la conexión del Almacén de Mensajes con los Clientes.

Específicamente el sistema observa la siguiente normativa:

- X.400 (1993) Message handling system and service overview. (ISO part 1)
- X.402 (1995) Overall architecture. (ISO part 2)
- X.407 (1988) Abstract service definition conventions. (ISO part 3)
- X.408 (1988) Encoded information type conversion rules
- X.411 (1995) Message transfer system: Abstract service definition and procedures (the definition of the P1 protocol). (ISO part 4)
- X.413 (1995) Message store: Abstract-service definition. (ISO part 5)
- X.419 (1995) Protocol specifications. (ISO part 6)
- X.420 (1992) Interpersonal messaging system. (ISO part 7)
- X.421 COMFAX use of MHS. (1994)
- X.435 (1991) Electronic data interchange messaging system. (ISO parts 8 and 9)
- X.460 Management model and architecture.

Cumplimiento con X.500

El servidor de directorio cumple las siguientes especificaciones X.500 de Internet.

ITU X.500	Overview of concepts, models and services, ISO/IEC 9594-1, 1993
ITU X.501	Models, ISO/IEC 9594-2, 1993.
ITU X.509	Authentication framework, ISO/IEC 9594-8, 1993.
ITU X.511	Abstract service definition, ISO/IEC 9594-3, 1993.
ITU X.518	Procedures for distributed operation, ISO/IEC 9594-4, 1993.
ITU X.519	Protocol specifications, ISO/IEC 9594-5, 1993.
ITU X.525	Replication, ISO/IEC 9594-9, 1993.

Las Declaraciones de Conformidad de Implementación de Protocolos (PICS) son documentos formales que describen cómo las versiones particulares de productos implementan en realidad lo definido por las normas de ISO/ITU. La Administración puede usar los PICS para determinar el cumplimiento de especificaciones y como interactuará el sistema con productos de otros vendedores. Nuestros sistemas se proveen con los PICS que cubren la normativa especificada.

Este documento lista todos los PICS publicados para M-Vault, M-Switch y M-Store.

M-Vault X.500 PICS.

Directory Access Protocol (DAP) - X.500(1993).

Directory System Protocol (DSP) - X.500(1993).

Directory Information Shadowing Protocol (DSIP)- X.500(1993).

M-Switch X.400 PICS

Common Messaging: Message Transfer (P1) - AMH11.

IPM: Requirements for Message Transfer (P1) - AMH22 Supplemental.

M-Store X.400 PICS

Common Messaging: MS Access (P7) - AMH13.

IPM: Requirements for enhanced MS Access (P7) - AMH24 Supplemental.

Soporte de protocolos de capa OSI baja o capas de transporte.

V. SOPORTE TÉCNICO

Concepto de apoyo y soporte técnico:

Se define el sistema de soporte al cliente a través de una Mesa de Ayuda disponible 24x7 y soporte en línea. Para obtener un soporte 24x7 eficaz, el cliente debe preparar un acceso de banda ancha en los servidores, disponible para los propósitos de soporte especializado. Este acceso estará equipado con un firewall dedicado en un CPU sin acceso (provista en el marco del contrato) y de esa forma se dejará habilitada la supervisión real “en línea” y el soporte del sistema, ambos servicios realizados remotamente por personal de nuestra empresa.

Este acceso permite a nuestro personal técnico supervisar en línea el sistema, reproducir algún fallo del mismo en nuestros laboratorios y poner el sistema bajo vigilancia y supervisión continua para que cualquier "condición de alarma" que se descubra en el sistema de monitoreo sea prontamente resuelta.

El personal que será dedicado al mantenimiento del sistema de mensajería tiene amplios conocimientos sobre este tipo de sistema.

El pedido de reclamo relacionado con el soporte técnico se realizará mediante envío de un Fax, llamada telefónica o mail donde se dejará constancia de la hora y tipo de evento ocurrido.

En el caso de que se necesite un cambio de la configuración, o si un operador experimenta dificultades y requiere ayuda, nuestras terminales están provistas con un portal remoto que, una vez que es habilitado por el operador, permite operar y configurar la Terminal remotamente.

El entrenamiento está orientado y basado en “entrenar a entrenadores” para permitirle al cliente que distribuya los conocimientos a través de su organización. Entendemos así que el cliente podrá ir gradualmente incrementando su participación en la instalación, configuración y mantenimiento del sistema en la medida que gane confianza en su propia habilidad.

Se proveerá un juego completo de documentos que entregan los fabricantes de los productos (COTS) y también de aplicaciones específicas por parte de nuestra empresa.

El sistema está concebido como un sistema modular de arquitectura abierta basada en productos COTS. Se espera que el ciclo de vida del sistema sea por consiguiente mucho mayor que quince años, dependiendo de las nuevas tecnologías del hardware y su reemplazo.

Renovación de tecnología: como propietario y desarrollador de las aplicaciones del software aeronáutico, el oferente está en capacidad de garantizar que las actualizaciones se desarrollarán y serán sin costo durante el período de prestación del servicio.

El servicio incluye:

La asignación de un equipo de soporte al cliente, incluyendo un administrador de cuenta y un supervisor de calidad en el centro de respuestas

Consejos operativos y técnicos.

Revisiones de la actividad de soporte.

Revisiones de la planificación de soporte.

Estudio medioambiental del sitio.

Valoración, una vez cada seis meses, del estado del sistema.

Análisis y administración de reparaciones del sistema operativo.

Actualizaciones del software.

Asistencia en la planificación de la capacitación.

Cobertura 24x7 para hardware y software en las siguientes condiciones:

Devolución de llamada en 2 horas en caso de problemas del software.

Respuesta en el sitio en 4 horas para prioridades 1 y 2 para el caso de problemas en el hardware.

Sistema de llamada flexible y administración escalable del mantenimiento según se verifique el estado de “prioridad del evento”.

Repuestos y Materiales:

Los repuestos y materiales serán los necesarios para mantener el sistema SMHS en servicio y su provisión será sin limitación y sin cargo durante el período de garantía, en tanto y en cuanto su recambio no se realice por una mala operación o trato indebido del equipo.