

How to

Q-expeditive Publicación vía Internet



Versión: 2.0

Fecha de publicación 11-04-2011

Aplica a: Q-expeditive 3

Índice

Introducción.....	3
Publicación de servicios	3
Ciudadanos.....	3
Terminales de auto consulta.....	3
Auto consulta vía Internet	4
Notificaciones vía SMS.....	5
IVR (Consulta telefónica).....	5
Distribución geográfica	6
VPN.....	6
Conexión segura con certificados	6
Inicio remoto.....	8
Correo electrónico	8
Web services	8
Conclusión.....	9

Introducción

El presente documento describe las posibilidades y la configuración necesaria para brindar los servicios de Q-expeditive a un público más amplio vía Internet.

Se dividirá el documento en dos escenarios funcionales, que son, la publicación de los servicios de consulta a los ciudadanos interesados en los trámites, permitiendo que los mismos puedan acceder a la información del estado del trámite en cualquier momento, y la extensión de los servicios de expediente electrónico a dependencias de la organización que se encuentran fuera de la intranet y separadas geográficamente, a entender, sucursales, organismos relacionados, etc.

Publicación de servicios

Para la publicación de servicios se definirán configuraciones para permitir el acceso a información de Q-expeditive por medio de Internet. Para cada caso se especificará la arquitectura y los requisitos físicos de conexión tanto para el cliente como para el servidor.

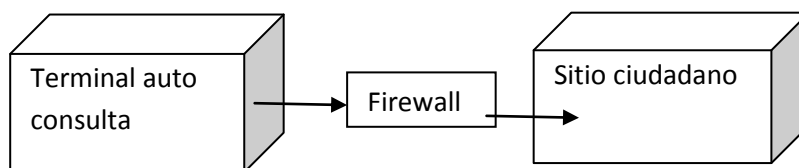
Ciudadanos

La publicación de servicios a ciudadanos implica permitir a los ciudadanos consultar el estado de un trámite de su interés en cualquier momento. Q-expeditive presenta un esquema en el cual se permite la impresión de un comprobante de inicio de trámite que puede ser entregado al ciudadano y que permite que el mismo consulte la información del trámite en forma segura utilizando un identificador único de trámite y una contraseña compleja autogenerada.

Para dicho esquema se presentan a continuación diversas alternativas.

Terminales de auto consulta

La forma más simple de permitir que un ciudadano consulte la información correspondiente a un trámite es ofreciendo en el lobby del organismo terminales de auto consulta, dichas terminales deberán contar únicamente con un navegador y pueden estar restringidas a la conexión únicamente con el sitio de auto consulta.



Para lograr este esquema se requiere una PC que funcione como Terminal de auto consulta y una conexión a la Red de Área Local (LAN) para que esta terminal acceda al sitio del ciudadano. Los requisitos de hardware para esta estación son los recomendados para poder utilizar el navegador.

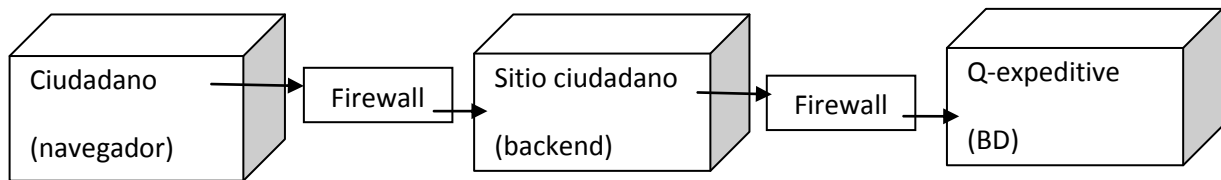
Patterns & Practices

En este esquema es importante tener cuenta las siguientes restricciones de seguridad:

- La terminal de auto consulta puede funcionar en forma de quiosco. No se requiere que el usuario acceda a ninguna opción fuera de la página de inicio del sitio de auto consulta.
- El usuario logueado a la máquina de auto consulta no debe ser administrador local de la máquina, de hecho sus privilegios se deben restringir al mínimo, permitiendo únicamente el uso del navegador y no permitiendo la edición de configuraciones ni instalación de software.
- El usuario logueado a la máquina de auto consulta no requiere ser un usuario del dominio, puede tratarse de un usuario local ya que el acceso al sitio de auto consulta utiliza seguridad de formularios (no requiere seguridad integrada). Manteniendo la máquina fuera del dominio se puede lograr una mayor restricción de los recursos del dominio a los cuales se desea que la máquina acceda.
- Se puede restringir, por ejemplo por medio de políticas de seguridad de un proxy (por ejemplo un ISA Server), el acceso a la red de la máquina que funciona como terminal de auto consulta restringiendo la navegación exclusivamente al sitio de auto consulta.

Auto consulta vía Internet

Para lograr que los ciudadanos interesados en los trámites puedan acceder a la información del trámite en cualquier momento, independientemente de su locación geográfica, una alternativa es la publicación del sitio de auto consulta a través de internet.



Para lograr este esquema se requiere que el ciudadano cuente con una conexión a internet de al menos 128kbps de bajada, y un navegador con el cual acceder al sitio de auto consulta. El sitio de auto consulta deberá publicarse en una dirección de internet, pudiéndose utilizar un dominio cualquiera o un subdominio de un dominio existente ya manejado por la institución (p. ej.: autoconsulta.institucion.org). La publicación del sitio web deberá realizarse sobre una IP pública fija a la que apunte el nombre correspondiente y podrá utilizarse una IP compartida, no se requiere contar con una IP única para la publicación del servicio, si no que puede utilizarse una IP que ya se utiliza con otros fines. Para la publicación del sitio institucional se recomienda reservar como mínimo 128kbps de subida, pero esto debe ajustarse según la cantidad de tráfico esperado que deberá estimarse según la realidad de la institución y el interés de los ciudadanos en consultar los trámites. La máquina que contiene el sitio de auto consulta puede ser virtualizada y presenta requisitos mínimos de hardware (PIV - 512 RAM)

Es importante tener en cuenta en este esquema los siguientes puntos con respecto a la seguridad:

- Solo se expone el sitio web de auto consulta a internet en una dirección pública. Las funcionalidades de este sitio son limitadas y solo permite consultas sobre trámites.
- Q-expeditive maneja un esquema de seguridad que limita al sitio de auto consulta a solo consultar información sobre trámites en el sistema. Esta información solo puede accederse mediante el identificador y el código de seguridad del trámite que se imprime en el momento de iniciar el mismo.
- El usuario del servicio del sitio de auto consulta puede limitarse, no requiriéndose que sea administrador local de la maquina expuesta a internet, y limitando las facultades sobre la base de datos de Q-expeditive, permitiendo por permisos de SQL que solo pueda tener acceso de lectura a las tablas del sistema.
- Se debe configurar los firewalls correspondientes para limitar el acceso a la máquina expuesta a Internet exclusivamente por el puerto 80 y sólo permitiendo la salida a la consulta de información contra la base de Q-expeditive con un usuario con privilegios limitados.
- Se recomienda que la máquina expuesta a internet cumpla esta función exclusivamente y se evite la instalación/habilitación de otro tipo de software que permita la entrada a intrusos o vulnerabilidades con respecto al acceso remoto.

Notificaciones vía SMS

Q-expeditive provee la capacidad de enviar notificaciones vía correo electrónico o vía SMS.

Adicionalmente se puede brindar la capacidad de consulta de trámites vía SMS. Este tipo de consulta requiere integrarse con un proveedor de telefonía celular o SMS y realizar la integración entre los servicios del proveedor de SMS y los servicios de Q-expeditive para poder validar las consultas del usuario y responder con la información correspondiente.

La recepción y envío de SMS contiene aspectos tecnológicos y económicos que varían según el proveedor seleccionado y que no se analizarán en el presente documento.

IVR (Consulta telefónica)

El IVR (consulta telefónica) permite que ciudadanos consulten por medio de teléfono, en forma auditiva, los trámites sobre los cuales tienen interés. Se permite la consulta del estado de los trámites seleccionando opciones luego de llamar a un número telefónico dado. Para realizar estas consultas se requiere contar con un proveedor de Text2Speech (lectura de mensajes al ciudadano) y con un servicio telefónico dedicado. Una vez instalado el sistema de IVR, el mismo puede ser utilizado con otros fines informativos, no requiere uso exclusivo por parte del sistema de expediente electrónico.

La conversión de texto a voz y la configuración del sistema de IVR contienen aspectos tecnológicos y económicos que varían según el proveedor y la tecnología seleccionada y que no se analizarán en el presente documento.

Distribución geográfica

Cuando se cuenta con sucursales u oficinas del organismo distribuidas geográficamente es deseable el expandir las bondades de un sistema de expediente electrónico fuera de los límites de la red de área local de la empresa (LAN). Dependiendo el escenario y la organización es posible que las sucursales y oficinas tengan acceso a la LAN por medio de tecnologías como el Frame Relay, pero no es necesario llegar a la implementación de tecnologías de tan alto costo para lograr la distribución geográfica del expediente electrónico, siendo posible hacer llegar el sistema a cualquier trabajador en cualquier localidad, siempre y cuando cuente con una conexión básica a internet (p ej. ADSL)

VPN

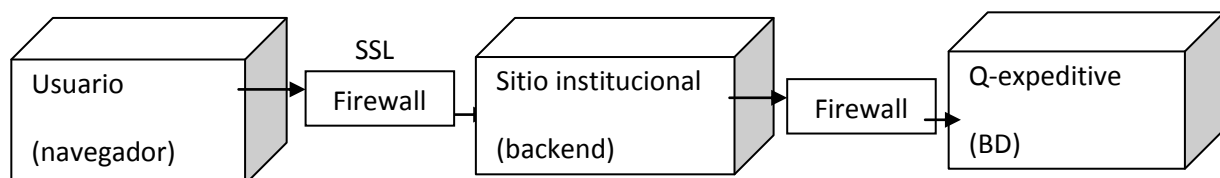
Si se cuenta con ancho de banda suficiente y se desea que los usuarios en puntos geográficamente distribuidos tengan acceso a otros recursos de la LAN, es posible que sea interesante el uso de una VPN. Si existe actualmente una VPN el acceso de los usuarios a los sistemas electrónicos son transparentes ya que podrán acceder a los servicios de expediente electrónico igual que cualquier otro trabajador que se encuentre dentro de la LAN.

Sin embargo, cabe resaltar que si el objetivo es simplemente hacer llegar la tecnología de expediente electrónico a puntos geográficos distribuidos, la implementación de una VPN resulta ser de una complejidad mayor que soluciones más simples (como la conexión segura mediante certificados que se detalla a continuación), puede desembocar en la exposición de recursos de la LAN que no se desean exponer y puede generar un consumo excesivo de ancho de banda.

Conexión segura con certificados

Cuando lo que se requiere es la publicación de los servicios de expediente electrónico para su uso desde locaciones geográficamente distribuidas, permitiendo el acceso al sistema a usuarios que se encuentran fuera de la LAN, podemos realizar la publicación del Sitio Institucional de Q-expeditive a través de Internet en forma segura.

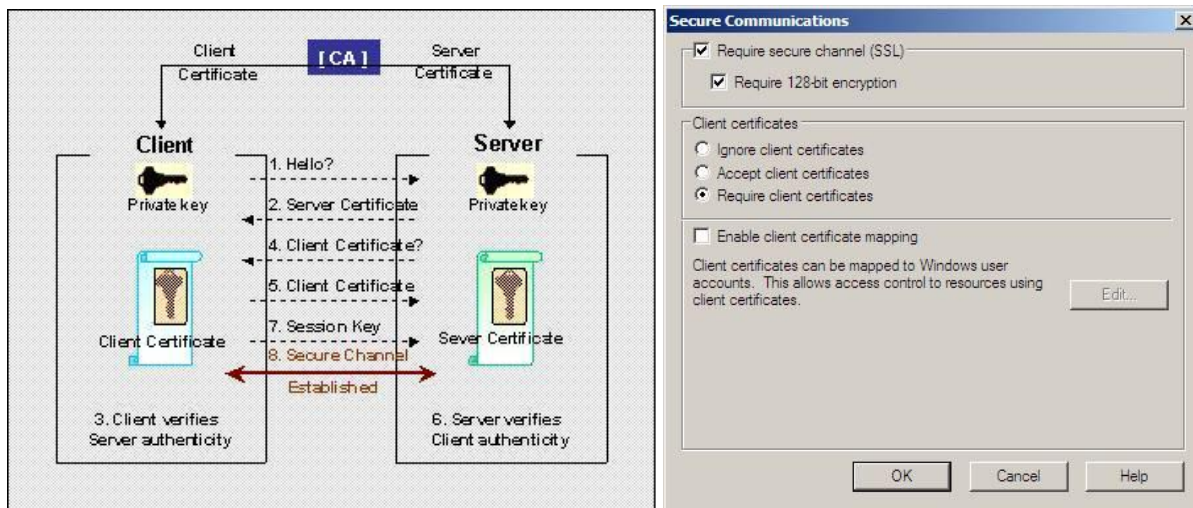
Para poder permitir el acceso al sitio de Q-expeditive de forma que el usuario trabaje con el sistema tal como si estuviera en el propio organismo se requiere que el usuario cuente como mínimo con una conexión de 512kbps de bajada y 128 de subida. El sitio Web Institucional deberá ser publicado en un dominio o subdominio de la institución (p ej.: expediente.organismo.org) y podrá utilizar una IP compartida. En este escenario el ancho de banda que se reserve para la publicación del servidor a Internet debe ser como mínimo de 256kbps de subida y deberá evaluarse el funcionamiento en función de la cantidad de usuarios concurrentes y el manejo de documentos adjuntos que se realicen en los trámites que son expuestos para uso mediante internet.



Patterns & Practices

La máquina que contenga el sitio Institucional a publicar puede ser virtualizada y presenta requisitos mínimos de hardware (PIV - 512 RAM), que pueden aumentar dependiendo de la cantidad de usuarios que accedan remotamente al sistema.

Para poder publicar en forma segura el servicio de expediente electrónico, se sugiere el uso de certificados electrónicos para validar la identidad de los usuarios que acceden al sistema. El sitio Institucional deberá ser expuesto utilizando SSL y requiriendo certificados por parte de los usuarios que se conecten. Dichos certificados deberán ser distribuidos a los distintos usuarios del organismo que requieran o deseen trabajar con el sistema en forma remota. El uso de SSL asegura que el acceso al servicio de expediente electrónico sólo puede ser accedido por usuarios de la organización en posición del correspondiente certificado digital. Toda la comunicación entre el cliente y el servidor se ve encriptada asegurando que la información enviada sólo pueda ser recibida por el servidor y la información recibida solo pueda ser accedida por el usuario en posesión del certificado digital.



Para el manejo de certificados, es posible que todos los certificados utilizados para manejar la autenticación sean certificados generados por una entidad certificadora local a la organización, eventualmente puede hacerse uso de la entidad certificadora de Windows Server.

Una vez generados los certificados y distribuidos entre los diferentes usuarios del sistema, se puede definir un usuario para cada uno en el Servicio de Directorio de la organización (p ej. LDAP) y mapear el certificado otorgado a un usuario del dominio. De esta forma el usuario que se autentica con el certificado contra el sitio Institucional de Q-expeditive se registra con las credenciales de un usuario del dominio que lo representa y el registro de las acciones del usuario se realiza como si el usuario fuera un usuario más del dominio.

Es importante tener en cuenta en este esquema los siguientes puntos con respecto a la seguridad:

- Se debe configurar los firewalls correspondientes para limitar el acceso a la máquina expuesta a Internet exclusivamente por el puerto 80 y sólo permitiendo la salida hacia la base de datos de Q-expeditive.

- Se puede limitar al usuario que ejecuta en el backend limitando las facultades del mismo. Es importante que este usuario tenga facultades limitadas sobre el sistema, sobre todo que no tenga acceso a recursos externos de la red fuera de la base de datos de Q-expeditive.
- Se recomienda que la máquina expuesta a internet cumpla esta función exclusivamente y se evite la instalación/habilitación de otro tipo de software que permita la entrada a intrusos o vulnerabilidades con respecto al acceso remoto.
- Los certificados digitales limitan el acceso de usuarios a los sistemas y se puede eventualmente limitar más el acceso al sitio web restringiendo desde cuales IPs se puede tener acceso. P ej., si los usuarios externos utilizan una conexión ADSL con IP fija, es posible limitar el acceso al sitio web institucional sólo a usuarios que acceden de esa IP. Esto implica una restricción mayor para evitar intentos de acceso no deseados, pero presenta limitaciones de acceso al sistema ya que limita a que usuarios que cuenten con IP variable debido a su acceso a la red no puedan trabajar con el sistema. Para estos escenarios se recomienda no utilizar el esquema de limitación de IP inicialmente y tomar el criterio de bloquear las IP desde las que se presentan posibles ataques al firewall.

Inicio remoto

Q-expeditive presenta adicionalmente una serie de alternativas para permitir el inicio de trámites a partir de eventos en distintos sistemas, incluyendo el correo electrónico. Estos esquemas permiten iniciar trámites pero se limitan a esto, no permitiendo la intervención posterior en el trámite de la persona que lo inicia.

Correo electrónico

Una forma de permitir que los ciudadanos o agentes externos inicien trámites es monitoreando una casilla de correo, de esta forma es posible que los correos electrónicos que lleguen a una determinada casilla realicen el inicio de un trámite en particular. Existe una limitación a este esquema ya que los datos del expediente que se reciban no contienen un formato en particular, pero puede utilizarse para los trámites que no requieran datos estructurados para su inicio.

Web services

En forma más genérica podemos hablar que de Q-expeditive publica Web Services que permiten que un evento en cualquier sistema externo inicie un trámite. Estos servicios son utilizados por ejemplo para el inicio mediante correo electrónico y pueden utilizarse en otros escenarios, por ejemplo inicio por medio de SMS o acciones en un portal Web público.

Conclusión

Q-expeditive cuenta con la estructura necesaria para brindar las funcionalidades de expediente electrónico por medio de Internet en forma segura. Tanto para ciudadanos interesados en un cierto trámite o tipos de trámite, como para la publicación de servicios completos para el trabajo con expedientes por medio de Internet orientado a funcionarios que se encuentren en lugares geográficos distantes o fuera de la LAN de la organización.

Los requisitos mínimos para el uso de estos servicios son de un Browser en el cliente (IE o Firefox) con los requisitos de Hardware mínimos del Browser utilizado y de una máquina con 512 de RAM para el servidor, que puede ser virtualizada, funcionando como servidor Web dedicado a la publicación de estos servicios.

Los requisitos de conexión a Internet para la publicación del sistema son de 128kbps para la publicación del sitio de auto consulta del ciudadano y de 256kbps de subida para la publicación del sitio institucional para el trabajo con expedientes. Se requiere como mínimo una IP fija, que puede ser compartida, y un nombre de dominio público sobre el cual se puedan crear subdominios.

Para los usuarios del organismo que interactúen con el sistema a través de Internet se sugiere como mínimo una conexión de 512/128kbps y se recomienda una conexión de 1Mbps/256kbps.