TECHNOLOGY

INNOVATION

<ECM/SEGURIDAD>

¡Ahora Seguridad!

Enterprise Content Management - ECM

DENTRO

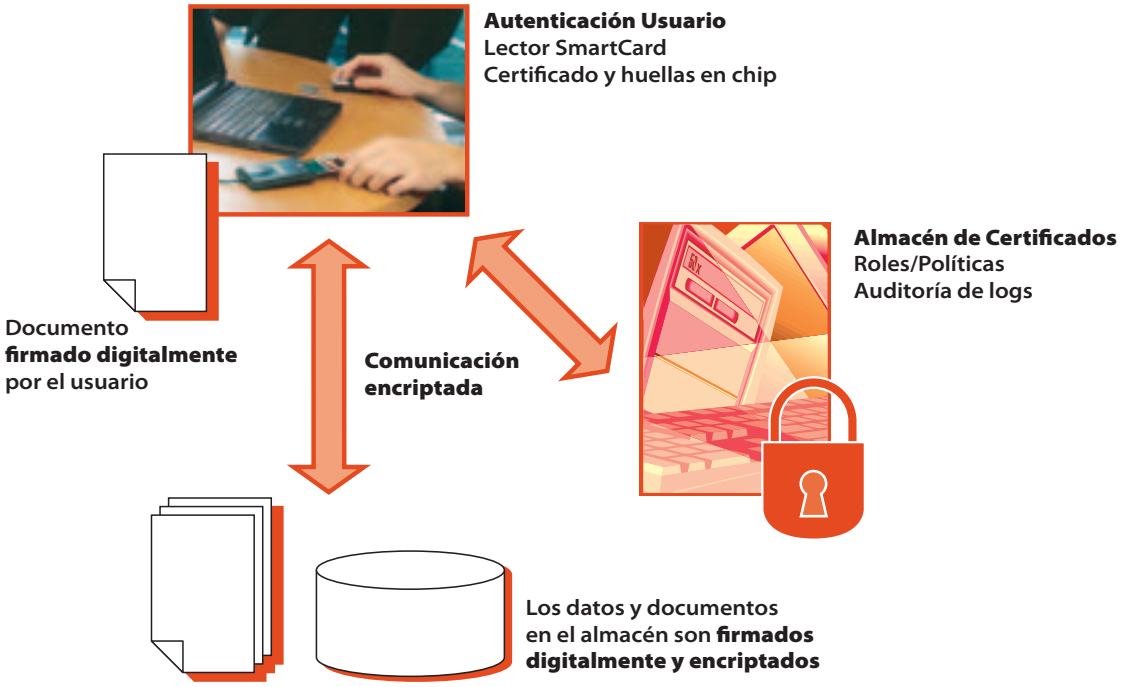
ISIS Papyrus proporciona aplicaciones ECM con la primera plataforma de la industria con sistema de seguridad integrado.

- Obtener la conformidad en la regulación de los documentos electrónicos.
- Las compañías pueden reforzar sus políticas de seguridad y evitar errores humanos o de fraude.
- Proporcionar Firma Digital para la aprobación del flujo de trabajo.
- Asegurar la confidencialidad de los documentos y la integridad del archivo a largo plazo.
- Autentificación y encriptación en las comunicaciones e-mail.

Control y Seguridad de Documentos

Papyrus Document System proporciona un control perfecto sobre cómo, cuándo y quién ha capturado, creado, accedido, cambiado, borrado y archivado los documentos. Las ventajas de usar la seguridad de Papyrus son:

- Reducción de riesgos potenciales en los datos
- Productividad en todas las aplicaciones de documentos
- Procedimientos de log-on simplificados
- Reducción considerable del coste para asegurar la regulación de conformidades



La autenticación es equivalente a mostrar el permiso de conducir en el mostrador de facturación del aeropuerto. Se usa para identificar quién, por ejemplo, ha firmado un documento en un proceso de negocio. Muchos países han validado legalmente el uso de Firmas Electrónicas, como hizo EEUU en octubre de 2000. La regulación normalmente no especifica la tecnología de firma digital, pero muchos expertos consideran que Public Key Infrastructure (PKI) desempeñará un papel destacado.

La funcionalidad de ***autenticación con usuario SmartCard*** de Papyrus proporciona la autenticación segura. Para hacer logon a Papyrus con la tarjeta (autenticación por posesión), además de un PIN (autenticación por conocimiento) o identificación de huella digital biométrica opcional (autenticación por identidad). La autenticación del logon normalmente consigue asegurando una política de claves. Ello conlleva una longitud mínima de clave, una complejidad mínima de clave, asegurar la duración de la clave y prohibir la reutilización de la clave cuando sobrepase el tiempo de inactividad. Todo ello no impide a los usuarios escribir claves o compartirlas con otros. Tampoco es posible asegurar la identidad del administrador. Muchas aplicaciones existentes usan transferencias de claves, y el login centralizado tiene problemas de red.

Usar una ***SmartCard con lector de huella*** digital asegura la identidad del usuario y refuerza la conformidad sin posibilidad de error humano. Una vez que la tarjeta se saca del lector, todas las aplicaciones Papyrus (opcionalmente la workstation) se bloquean. El certificado de usuario y la huella digital se almacenan de forma segura en la tarjeta y no se requiere una posterior autenticación para acceder a la red.

Los siguientes conceptos se implementan con Papyrus:

Autenticación: Asegurar que un usuario es identificado con certeza.

Confidencialidad: Encriptar el documento y las transmisiones de datos.

Autorización: Controlar lo que alguien puede hacer con documentos o workflow.

Responsabilidad: Hacer seguimiento de lo que alguien hizo con un documento.

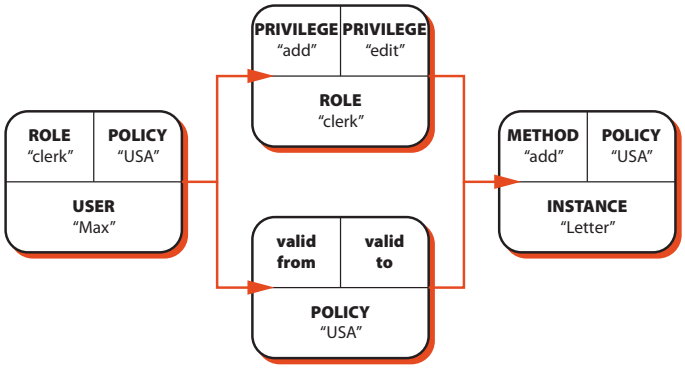
Autenticidad: Verificar la originalidad y fuente de un documento.

Auditoría: Ser capaz de crear un registro de conformidad completo.

La confidencialidad se asegura en Papyrus encriptando las transmisiones de datos y todos los objetos de datos almacenados. Para aplicaciones web Papyrus usa HTTPs, la versión segura de HTTP, el protocolo de comunicación de la World Wide Web. Proporciona autenticación y comunicación encriptada para el acceso al navegador o a un servidor WebPortal.

La autorización define lo que una persona, una vez identificada, puede hacer con una aplicación o recurso del sistema. Está determinado por ser miembro de un grupo particular. Papyrus Objects usa un sistema de autorización integrado, para asegurarse de que ningún usuario o programa acceda o haga algo sin la autorización pertinente.

Una vez que la organización corporativa está definida, no es necesario definir roles de la aplicación que se implementará con Papyrus.



Cada usuario recibe al menos un ROL. Dicho ROL ha definido bien una serie de privilegios o un método para un objeto. Para definir a qué INSTANCIAS de los recursos tiene acceso un usuario, se necesita POLITICA de autorización, que ha de ajustarse a la POLITICA definida para el objeto. El usuario tiene permiso para ejecutar un método de un tipo particular, pero sólo tiene permiso para acceder a este tipo de un departamento específico. Papyrus LDAP Adapter permite el uso de roles de usuario existentes disponibles en directorios tanto LDAP, como RACF.

La Responsabilidad (Accountability) se logra con la combinación de autenticación de usuario y parametrización de las funciones de auditoría para un workflow y sus documentos relacionados. Como ha identificado al usuario con su SmartCard y huella digital, su ROL y POLÍTICA aseguran que puede acceder, y todas las actividades del usuario también pueden ser escritas en un log auditor. Así el usuario puede, en cualquier momento, ser responsable de sus acciones. Esto es muy importante para los Administradores de Seguridad del Sistema, Administradores de Gestión de Cambios, Directores de Producción o usuarios que dan la aprobación a las aplicaciones o a los cambios de documentos.

Autenticidad: una vez que un documento se convierte en un registro corporativo o logra un estatus legal como parte de un contrato, el estado del workflow cambia y el documento se encripta y firma digitalmente. El documento ya sólo podrá ser abierto por las partes autorizadas sin necesidad de almacenarlo en un medio de sólo de escritura. Sólo los usuarios que tengan autoridad para acceder a la "public key" del documento pueden realmente leerlo.

Auditing Analysis Output

Auditar es hacer el seguimiento de la actividad por los usuarios así como por la definición de sistemas. La información almacenada permite a los usuarios autorizados hacer auditorías. Las auditorías típicas son relativas a cambios de las definiciones de seguridad o a qué documento se ha enviado y quién accedió a él. Esto se realiza usando funciones de seguridad tales como autenticación y logging de datos. El diseño estándar de documentos con Papyrus, funcionalidades de planificación y distribución controlan cuándo y qué informe es formateado, cómo y a quién se distribuye.

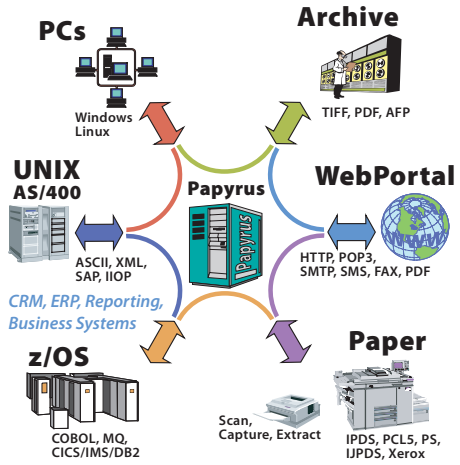
MOTIVACION *para* INNOVAR

Motivación: Conformidad con la regulaciones de privacidad y mantenimiento de registros

Innovación: Integración de seguridad total en ECM con autenticación SmartCard

Solución: Funciones de seguridad de la plataforma Papyrus Document Switchboard

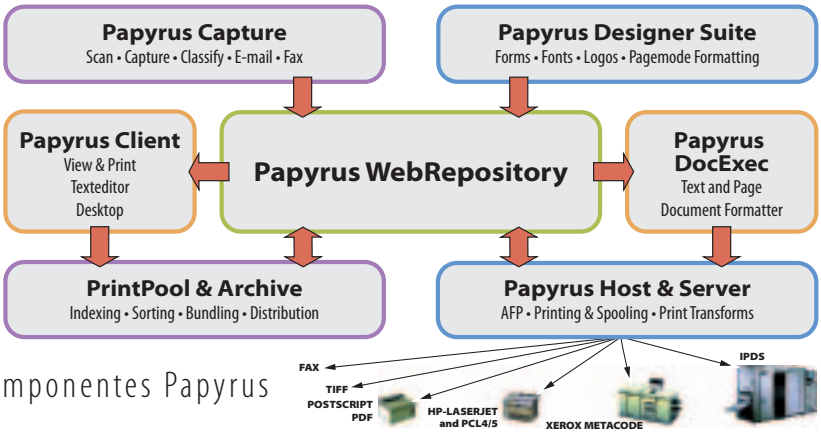
Una **solución global y escalable** para gestión centralizada de aplicaciones de documentos, impresión y operaciones de salida que abarcan entornos web, cliente/servidor y host.



Papyrus Document Frameworks

- Factoría Automatizada de Documentos
- Integración de Aplicaciones Corporativas
- Gestión de Salidas Corporativas
- Gestión de Contenidos Corporativos
- Gestión de Procesos
- Aplicaciones Portal y Web
- Gestión de Cambios
- Correspondencia
- Gestión de Campañas
- Gestión de Impresión
- Captura/Clasificación/Extracción
- E-mail, Fax

Las compañías pueden **definir, parametrizar, y gestionar** salidas en entornos complejos y heterogéneos, desde puntos de control centralizados.



Componentes Papyrus

Selección de entre más de 2000 Referencias ISIS Papyrus:

Sector Finanzas usan Papyrus

Citibank, Deutsche Bank, HFC Bank, UBS, Credit Suisse, BNP, Capital One, Lloyds TSB

Seguros usan Papyrus

Allianz, Generali, Thrivent, RAS, Great West Life, Sun Life, HBOS, Zürich , Hibernian

Salud usan Papyrus

AXA, HUK, Empire Health Choice, Siemens Medical Systems, Sanitas, Hallesche

Telecomunicaciones usan Papyrus

Bell South, SwissCom, T-Mobile, Debitel, Orange, Singapore Telecom, Belgacom

Sector Público usan Papyrus

EDS Department of Social Services, EDS Jobseeker, European Patent Office

Industria usan Papyrus

Avon Cosmetics, Bally Shoes, BASF, Canon, IKEA, Miele & Cie, Renault, Volkswagen

Oficinas ISIS

Austria (Oficina Central)

ISIS Information Systems GmbH
ISIS Marketing Service GmbH
ISIS Knowledge Systems GmbH
Alter Wienerweg 12
A-2344 Maria Enzersdorf

T: +43-2236-27551-0
F: +43-2236-21081
E-mail: info@isis-papyrus.com

Estados Unidos

ISIS Papyrus America, Inc.
301 Bank St.
Southlake, TX 76092

T: 817-416-2345
F: 817-416-1223

Asia-Pacífico

ISIS Papyrus Asia Pacific Ltd
9 Temasek Blvd.
#15-03 Suntec City Tower 2
Singapore 038989

T: +65-6339-8719
F: +65-6336-6933

España

ISIS Thot SL.
Sainz de la Calleja, 14
28023 Madrid

T: +34-91-307-78-41
F: +34-91-307-75-08

Gran Bretaña

ISIS Papyrus UK Ltd.
Watership Barn
Kingsclere Business Park
Union Lane, Kingsclere
Hants, RG20 4SW

T: +44-1635-299849
F: +44-1635-297594

Alemania

ISIS Papyrus Deutschland GmbH
Heerdter Lohweg 81
40549 Düsseldorf

T: +43-2236-27551-0
F: +43-2236-21081

Holanda

ISIS Papyrus Netherlands B.V.
WTC World Trade Center
Zuidplein 36
1077 XV Amsterdam

T: +31-20-799-7716
F: +31-20-799-7801

Italia

ISIS Papyrus Italy Srl
via Monte Navale 11
10015 Ivrea (TO)

T: +39-0125-6455-00
F: +39-0125-6455-150

Francia

ISIS Papyrus France SARL
21, Rue Vernet
75008 Paris

T: +33-1-47 20 08 99
F: +33-1-47 20 15 43

www.isis-papyrus.com