TECHNOLOGY INNOVATION

<ECM/SECURITY>

Security Now!

Enterprise Content Management - ECM

INSIDE

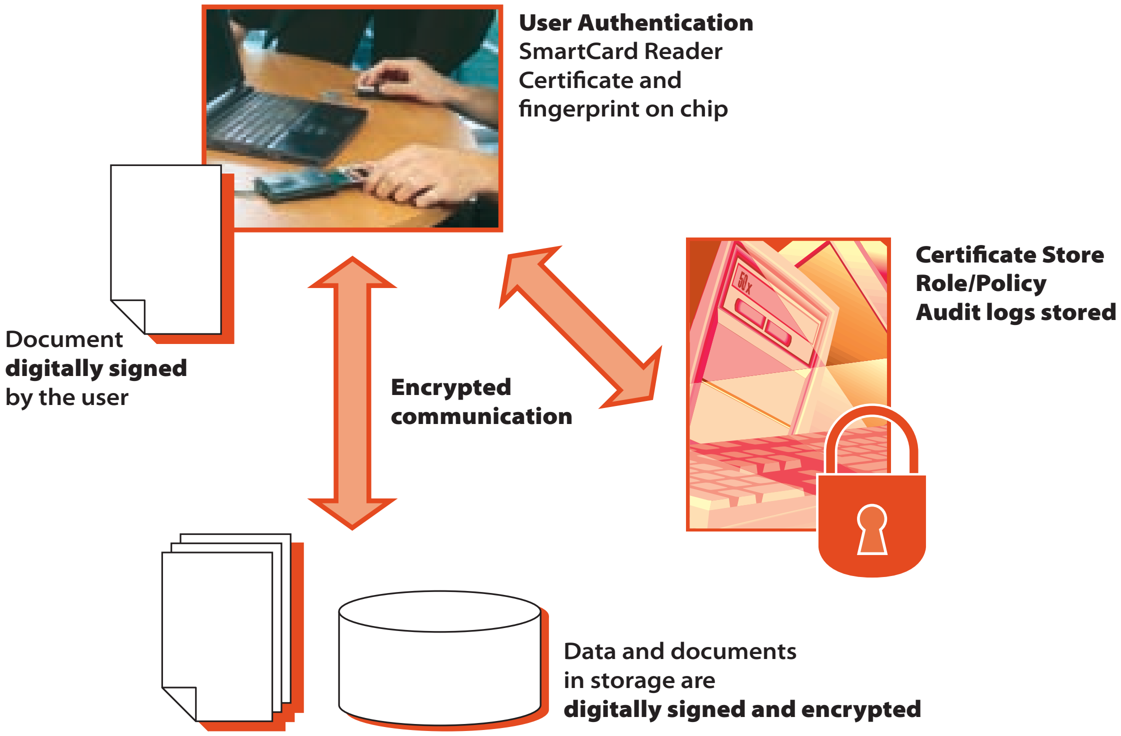
ISIS Papyrus provides ECM applications with the industry's first deep-integrated application and system security.

- Bringing privacy regulation compliance to electronic documents.
- Organizations can enforce corporate security policies and avoid human error or fraud.
- Provide Digital Signatures for Workflow sign-off.
- Ensure document confidentiality and long-term archive integrity.
- Authenticated and encrypted e-mail communication.

Document Control and Security

The *Papyrus Document System* provides perfect control over how, when, and by whom your documents are captured, created, accessed, changed, deleted and archived. The benefits of using Papyrus security are:

- Reduced potential damage risk
- Increased productivity across all document applications
- Simplified log-on procedures
- Substantially lower cost for ensuring regulatory compliance



Authentication is equivalent to showing your drivers license at the ticket counter at the airport. It is used to identify who has for example, signed a document in a business process. Many countries have legally validated the use of Electronic Signatures, as has the United States since October 1st, 2000. Regulation does usually not specify a digital signature technology, but many experts consider that Public Key Infrastructure (PKI) will play an important role.

The integrated ***SmartCard User Authentication*** functionality in Papyrus provides secure user authentication. To log on to Papyrus the card itself (authentication by possession) as well as a PIN (authentication by knowledge) or optional biometric fingerprint identification (authentication by identity). Logon authentication is usually achieved by trying to enforce a password policy. This involves requesting a minimum password length, minimum password complexity, enforced password aging, and prohibiting password reuse as well as inactivity time-outs. All this does not prevents users from writing passwords down or sharing them with others. The identity of the security administrator is also not ensured. Many existing applications use password transfers in clear text, and the central login creates issues with offline use or with network problems.

Using a ***SmartCard with fingerprint reader*** ensures a user's identity and enforces compliance without the possibility for human error. Once the card is pulled from the reader, all Papyrus applications (optionally the workstation) are locked out. The user certificate and fingerprint is securely stored on the card and thus authentication does not require network access.

The following security concepts are implemented in Papyrus:

Authentication: Ensure that a user is identified with certainty.

Confidentiality: Encrypt the document and data transmissions.

Authorization: Control what someone can do with a document or workflow.

Accountability: Track what someone did with a document.

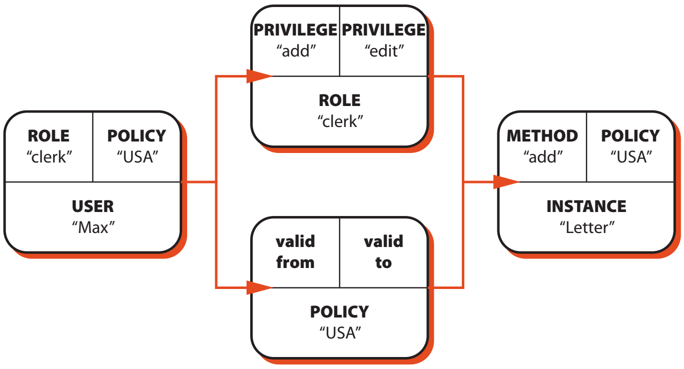
Authenticity: Verify the originality and source of a document.

Auditing: Being able to create a full compliance record.

Confidentiality is ensured within Papyrus by encrypting the data transmissions and all data objects stored. For Web applications Papyrus uses HTTPs, the secure version of HTTP, the communication protocol of the World Wide Web. It provides authentication and encrypted communication for browser access to a WebPortal server.

Authorization defines what a person, once identified, is permitted to do with an application or system resource. This is usually determined by being a member of a particular group, equivalent to checking for your ticket when you go to the theatre. Papyrus Objects uses an integrated authorization system, to ensure that no user or program can access or do anything without the proper authorization.

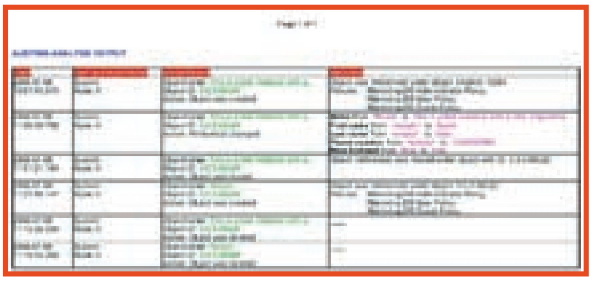
Once the corporate organization is defined in principle, the application roles to be implemented with Papyrus need to be defined.



Each user receives at least one ROLE. This ROLE has defined either a privilege string or an actual method of an object. To define which resource INSTANCES a user is allowed to access, also a POLICY authorization is needed, which has to match the POLICY defined for the object. The user may be allowed to perform a method for a particular type of letter, but is only allowed to access this type of letter of a specific department. The Papyrus LDAP Adapter allows the use of existing user roles available in LDAP directories, such as RACF.

Accountability is achieved by a combination of user authentication and setting up the auditing functions for a workflow and its related documents. As you have identified the user by his SmartCard and fingerprint, his ROLE and POLICY ensure what he can access, and all activities of the user can also be written into an audit log. Thus the user can at all times be held accountable for his actions. This is mostly important for System or Security Administrators, Change Management Administrators, Production Managers or users who sign off application or document changes.

Authenticity: Once a document becomes a corporate record or achieves a legal status as part of a contract, the workflow state is changed and the document is encrypted and digitally signed. The document can now only be opened by authorized parties and as long as the signature is intact, the authenticity of the original can be verified without the need for storing the document to Write-Only media. Only users who have the authority to access the private key of the document can actually read it.



Auditing Analysis Output

Auditing is the tracking of activity by users as per the systems definition. This stored information allows authorized users to conduct audits. Typical audits are related to changes in security definitions or which way a document was routed and who accessed it. This is accomplished by using security functions such as authentication and data logging. Standard Papyrus document design, scheduling and distribution features controls when and which reports are formatted how and distributed to whom.

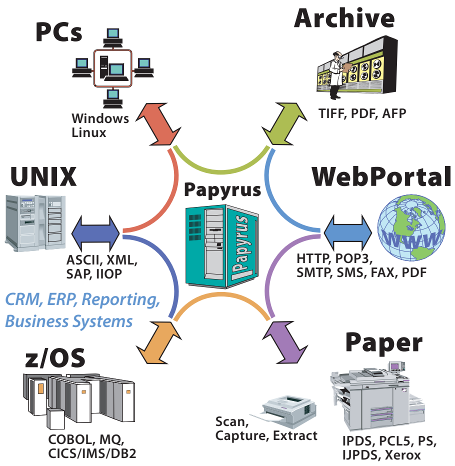
MOTIVATIONS *for* INNOVATION

Motivation: Compliance with privacy and record keeping regulations

Innovation: Full security integration for ECM with SmartCard authentication

Solution: Security functions of the Papyrus Document Switchboard

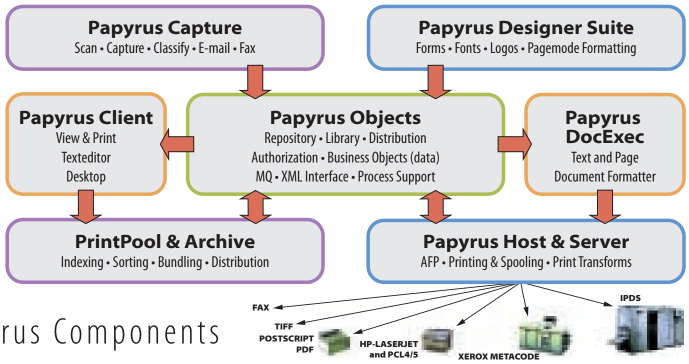
A comprehensive and scalable solution for centralized management of document applications, print and output operations that span web, client/server and host environments.



Papyrus Document Frameworks

- Automated Document Factory
- Enterprise Application Integration
- Enterprise Output Management
- Enterprise Content Management
- Business Process Management
- Portal and Web Applications
- Change Management
- Correspondence
- Campaign Management
- Print Management
- Capture/Classify/Extract
- E-mail, Fax

Organizations can define, measure, and manage output management across complex heterogeneous environments from centralized control points.



Papyrus Capture
Scan • Capture • Classify • E-mail • Fax

Papyrus Designer Suite
Forms • Fonts • Logos • Pagemode Formatting

Papyrus Client
View & Print
Texteditor
Desktop

Papyrus Objects
Repository • Library • Distribution
Authorization • Business Objects (data)
MQ • XML Interface • Process Support

Papyrus DocExec
Text and Page
Document Formatter

PrintPool & Archive
Indexing • Sorting • Bundling • Distribution

Papyrus Host & Server
AFP • Printing & Spooling • Print Transforms

Papyrus Components

A selection from over 2000 ISIS Papyrus References:

Finance Sector uses Papyrus

Citibank, Deutsche Bank, Commerzbank, UBS, Credit Suisse, BNP, Capital One

Insurance uses Papyrus

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

Healthcare uses Papyrus

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

Telecommunication uses Papyrus

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

Public Sector uses Papyrus

Commonwealth of Pennsylvania, European Patent Office, Stadt Düsseldorf

Manufacturing uses Papyrus

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

ISIS Locations

International Headquarters, Austria

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

US Headquarters

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

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

Asia-Pacific Headquarters

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

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

England

ISIS Papyrus UK Ltd
25 Cherry Orchard North
Kembrey Park
Swindon
Wiltshire SN2 8UH

T: +44-1793-644616
F: +44-1793-692978

Germany

ISIS Papyrus Deutschland GmbH
Heerdter Lohweg 81
40549 Düsseldorf

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

Benelux

ISIS Papyrus Benelux
Braine l´Alleud Parc de l´Alliance
9, Boulevard de France, bât A
1420 Braine l´Alleud

T: +32-2-352-8720
F: +32-2-352-8802

Italy

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

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

France

ISIS Papyrus France SARL
La Grande Arche Paroi Nord
92044 Paris La Défense

T: +33-1-40903510
F: +33-1-40903501

Spain

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

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

www.isis-papyrus.com