TECHNOLOGY

INNOVATION

<ECM/SÉCURITÉ>

Parlons Sécurité!

Enterprise Content Management - ECM

SOMMAIRE

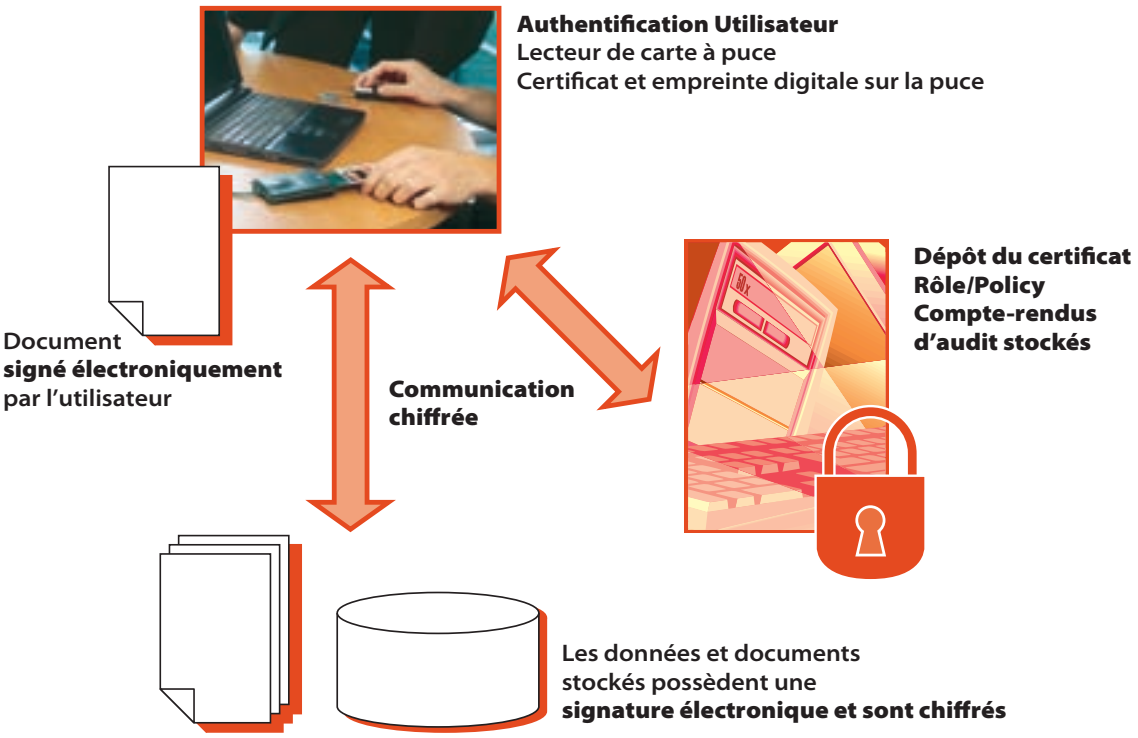
ISIS Papyrus fournit une solution de gestion de contenu (ECM) totalement intégrée au standard de l'industrie en matière de sécurité des systèmes et des applications.

- Respect des règles de sécurité pour les documents électroniques.
- Mise en œuvre des normes de sécurité définies au niveau de l'entreprise évitant ainsi toute fraude ou erreur humaine.
- Utilisation de signatures numériques pour la validation de Workflow.
- Garantie de la confidentialité du document et de l'intégrité des archives long-terme.
- Communication par mail authentifiée et chiffrée.

Contrôle et Sécurité du Document

Avec *Papyrus Document System* il est possible de suivre en permanence quand et par qui les documents ont été saisis, créés, consultés, modifiés, supprimés et archivés. Les avantages liés à l'utilisation des fonctions de sécurité de Papyrus sont:

- Réduction du risque potentiel de dommages.
- Productivité accrue sur toutes les applications documentaires.
- Procédures de log-on simplifiées.
- Diminution substantielle des coûts requis pour assurer la conformité en matière de contrôle.



L'authentification peut être comparée à la présentation d'un passeport dans un aéroport. Au sein d'une entreprise l'authentification permettrait d'identifier qui a validé un document. Dans de nombreux pays, l'utilisation de la signature électronique a été entérinée d'un point de vue légal. La législation ne préconise pas une technologie de signature électronique particulière, néanmoins la plupart des experts considèrent que l'infrastructure à clef publique (PKI) jouera un rôle important dans le domaine.

La méthode d'authentification via une carte à puce (SmartCard) constitue un moyen sécurisé d'accès aux systèmes. Pour s'identifier dans Papyrus, il est possible d'utiliser la carte elle-même (authentification par possession/détention), un PIN (authentification par la connaissance) ou optionnellement l'identification biométrique avec empreinte digitale (authentification par identité). L'authentification par log-on est caractérisée par la saisie d'un mot de passe. Ceci implique la mise en place de contraintes en terme de taille, de complexité, de durée de validité, de renouvellement, d'archivage des mots de passe ainsi que de règles de time-out de sessions. Il reste que cette méthode n'empêche pas les utilisateurs de consigner par écrit ces mots de passe et de les partager. L'identité de l'administrateur sécurité n'est pas non plus garantie. De nombreuses applications existantes utilisent les transferts de mots de passe en clair et l'utilisation d'un login central engendre des problèmes lors d'accès off line ou on-line.

L'utilisation d'une carte à puce (Smartcard) avec un lecteur d'empreinte digitale garantit l'identité de l'utilisateur, applique les règles en matière de conformité sans possibilité d'erreur humaine. Une fois la carte retirée du lecteur, toutes les applications Papyrus (voire les stations de travail) sont verrouillées. Le certificat utilisateur et l'empreinte digitale sont stockés de manière sûre sur la carte, de ce fait l'authentification n'exige pas l'accès au réseau.

Les concepts suivants en matière de sécurité font partie intégrante de Papyrus:

Authentification: Garantie qu'un utilisateur est identifié avec certitude.

Confidentialité: Chiffrement des transmissions de documents et de données.

Autorisation: Contrôle des droits d'une personne au niveau du document ou du workflow.

Responsabilité: Suivi des opérations effectuées par une personne sur un document.

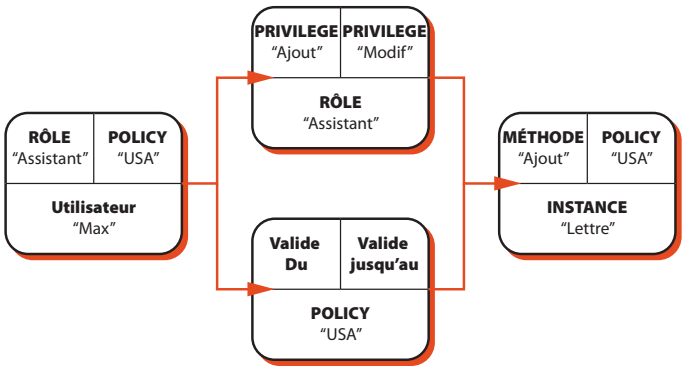
Authenticité: Vérification de l'originalité et de la source d'un document.

Audit: Possibilité de créer un rapport complet de conformité.

La confidentialité est assurée dans Papyrus via le chiffrement des transmissions de données et de tous les objets stockés. Pour les applications Internet, Papyrus utilise HTTPs, la version sécurisée de http, le protocole de communication d'Internet. Lors de l'accès au WebPortal Server via un navigateur, il fournit une authentification et une communication chiffrées.

L'autorisation détermine ce qu'une personne, une fois identifiée, peut faire avec une application ou une ressource système, en fonction de son appartenance à un groupe particulier. Papyrus Objects utilise un système intégré d'autorisation permettant de s'assurer qu'aucun utilisateur ou programme peut accéder à une donnée ou exécuter un traitement sans l'autorisation appropriée.

Les rôles à créer au sein de Papyrus doivent être définis en fonction de l'organisation interne de l'entreprise.



Chaque utilisateur dispose d'au moins un rôle. Ce rôle définit soit une chaîne de privilèges soit une méthode pour un objet. La notion de POLICY détermine à quelles instances d'une ressource un utilisateur a droit d'accès. Cette POLICY doit correspondre à celle définie pour l'objet. L'utilisateur peut être par exemple autorisé à exécuter une méthode pour un certain type de lettre mais ne peut accéder à ce type de lettre que pour un département particulier. L'adaptateur Papyrus LDAP permet l'utilisation des rôles utilisateurs déjà existants dans les annuaires LDAP tel que RACF.

La notion de responsabilité est la combinaison de l'authentification utilisateur d'une part et des fonctions d'audit définies pour un workflow et les documents s'y rapportant d'autre part. Dès lors que l'utilisateur a été identifié via sa carte à puce et son empreinte digitale, son rôle et sa POLICY déterminent ce à quoi il a accès et toutes les opérations qu'il fera seront tracées. Ainsi à tout moment l'utilisateur peut être tenu responsable de ses actions. Cette notion est importante pour les administrateurs système, les responsables sécurité, les responsables de production ou les utilisateurs qui valident les modifications apportées aux documents ou aux applications.

Authenticité: Une fois que le document devient un document d'entreprise ou revêt un caractère légal en tant qu'élément d'un contrat par exemple, l'état du workflow est modifié, le document est crypté et protégé par une signature électronique. Dès lors, il ne pourra être ouvert qu'aux conditions suivantes : les personnes autorisées doivent avoir accès à la clef publique et la signature doit demeurer intacte. L'authenticité de l'original peut être vérifiée sans avoir besoin de stocker le document sur un support en écriture seule.

Exemple de compte-rendu d'audit

L'audit est le suivi de l'activité par utilisateur en fonction de paramètres prédéfinis. Cette information stockée permet aux utilisateurs autorisés de procéder à des opérations de contrôle et de savoir par exemple si les règles de sécurité ont été modifiées, par quel biais le document a été transmis et qui y a eu accès. Ceci se fait au travers des fonctions de sécurité (authentification et traçage). Les fonctions standard de conception, de planification et de distribution de Papyrus contrôlent non seulement quels documents doivent être formatés mais aussi comment, quand et à qui ils doivent être restitués.

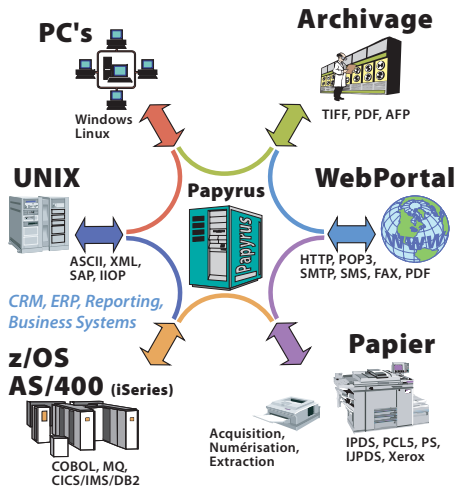
Objectifs *en matière d'*INNOVATION

Objectif: Conformité avec les règles en matière de confidentialité et de traçabilité

Innovation: Intégration complète de la sécurité au niveau ECM avec méthode d'authentification via carte à puce (SmartCard)

Solution: Les fonctions de Sécurité de Papyrus Document Switchboard

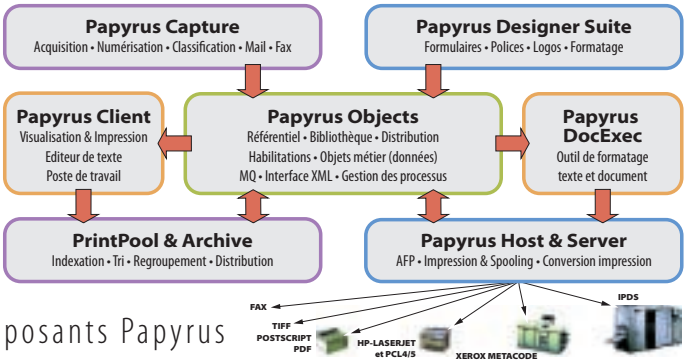
Une solution complète et évolutive pour la gestion centralisée des applications documentaires ainsi que les opérations d'impression et de restitution s'étendant de l'environnement Web aux environnements client/serveur et mainframe.



Papyrus Document Frameworks

- Automated Document Factory
- Enterprise Application Integration
- Enterprise Output Management
- Enterprise Content Management
- Business Process Management
- Applications Portail et Web
- Change Management
- Application courrier
- Gestion des campagnes
- Gestion des impressions
- Capture/Classification/Extraction
- Mails, Télécopies

Les organisations peuvent, à partir de points de contrôle centralisés, définir, mesurer et contrôler la gestion des restitutions au travers d'environnements hétérogènes complexes.



Les composants Papyrus

Quelques références parmi les 2000 clients ISIS Papyrus:

Papyrus dans le secteur bancaire

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

Papyrus dans le secteur de l'assurance

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

Papyrus dans le secteur de la santé

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

Papyrus dans le secteur des télécommunications

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

Papyrus dans le secteur public

Commonwealth of Pennsylvania, European Patent Office, Stadt Düsseldorf

Papyrus dans le secteur de l'industrie

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

Bureaux ISIS

Siège international, Autriche

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

Siège pour les USA

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

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

Siège pour la région Asie/Pacifique

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

Singapore 038989
T: +65-6339-8719
F: +65-6336-6933

Royaume-Uni

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

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

Allemagne

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

Italie

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
21, Rue Vernet
75008 Paris

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

Espagne

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