TECHNOLOGY

INNOVATION

<ECM/SECURITY>

INHALT

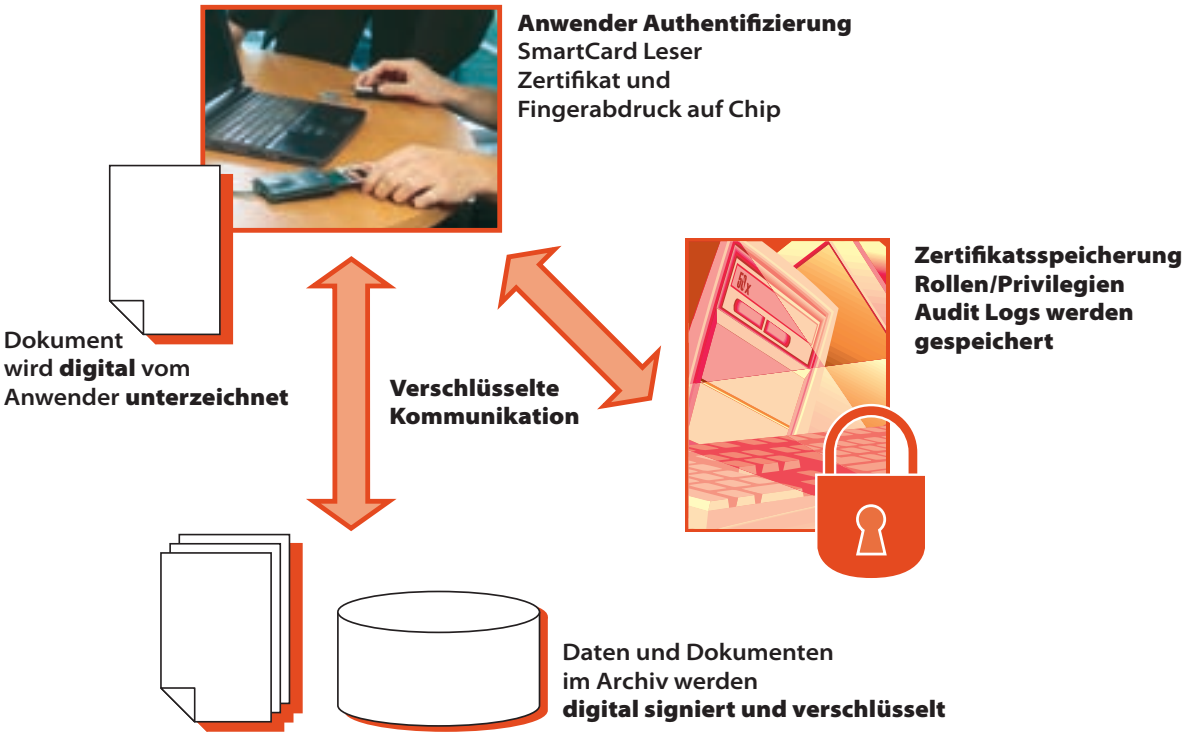
ISIS Papyrus offeriert das erste ECM System mit integrierter Sicherheitsfunktionalität.

- Einhaltung von Datenschutzbestimmungen für elektronische Dokumente
- Umsetzung unternehmensweiter Sicherheitsstandards
- Ausschließung menschlichen Irrtums oder Missbrauchs
- Verwendung digitaler Unterschriften in Geschäftsprozessen
- Garantierte Dokumentenvertraulichkeit und Langzeit-Archiv Integrität
- Authentifizierte and verschlüsselte E-Mail Kommunikation

Dokumenten Überwachung und Sicherheit

Mit dem *Papyrus Document System* kann nachvollzogen werden wie, wann und von wem Dokumente erfasst, erzeugt, gelesen, verändert, gelöscht und archiviert wurden. Die Nutzen der Papyrus Sicherheitsfunktionen sind:

- Verminderung möglicher Schäden durch Datenmissbrauch
- Gesteigerte Produktivität über Plattformen hinweg
- Benutzerfreundlicheres, einfaches Log-on
- Substantiell niedrigere Kosten bei der Umsetzung gesetzlicher Bestimmungen



Authentifizierung kann mit der Vorlage eines Lichtbildausweises verglichen werden. Sie dient dazu sicherzustellen, daß eine Person mit Sicherheit identifiziert wird. Log-on Authentifikation wird für gewöhnlich durch Einhaltung von Passwortregeln gewährleistet. Dies erfordert ein vorgeschriebenes Mindestmaß an Passwortlänge und Passwortkomplexität, zeitlich eingeschränkte Passwortgültigkeit, einmalige Passwortverwendung und Time-outs durch Benutzerinaktivität. All das verhindert nicht, daß Passwörter aufgeschrieben oder an Kollegen weitergegeben werden. Die in Papyrus integrierte Funktionalität der SmartCard User Authentifizierung bietet absolut sichere Identifikation der Person.

Um sich in Papyrus anzumelden, wird die ***SmartCard*** (Authentifizierung durch Besitz), ein PIN (Authentifizierung mittels Wissens) und optional biometrische Identifikation durch Fingerabdruck (Authentifizierung durch Identität) benutzt.

Auch die Identität des Sicherheits-, System-, oder Applikationsadministrators wird durch ***SmartCard*** und ***Fingerabdruck*** gewährleistet. Wird die SmartCard aus dem Lesegerät entnommen, sind alle Papyrus Anwendungen oder optional auch die Arbeitsstation gesperrt. Da das Benutzerberechtigungszertifikat und der Fingerabdruck sicher auf der SmartCard gespeichert sind, benötigt der Nutzer für eine Authentifizierung keine aktive Netzwerkverbindung. Bei einem ausschließlich zentral verwalteten Log-on kann es zu Problemen bei Off-Line Nutzung oder bei Netzwerkstörungen kommen.

Die SmartCard Technologie von Papyrus kann auch für die elektronische Unterschrift genutzt werden. In vielen Ländern wird die elektronische Unterschrift bereits als rechtsverbindlich anerkannt. Meist definiert die Gesetzgebung nicht die Technologie der digitalen Unterschrift, jedoch wird die Public Key Infrastructure (PKI), wie sie auch in Papyrus benutzt wird, eine bedeutende Rolle spielen.

Folgende Sicherheitskonzepte sind in Papyrus implementiert:

Authentifikation: Sichere Identifikation des Benutzers.

Vertraulichkeit: Verschlüsselung des Dokuments und der Datenübertragung.

Autorisierung: Überwachung der Zugriffsrechte auf Dokumente und Anwendungen.

Zurechenbarkeit: Benutzerbezogene Nachvollziehbarkeit von Prozessen.

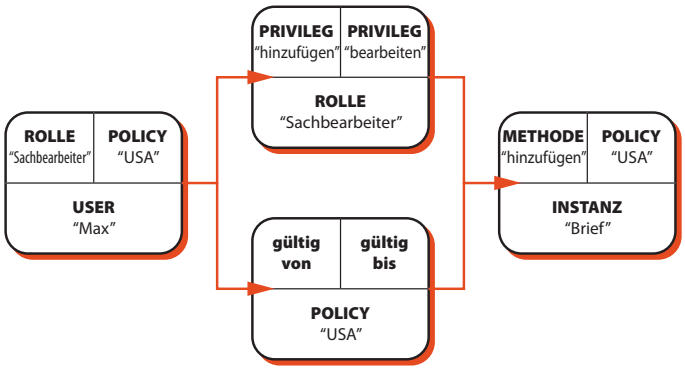
Authentizität: Überprüfung der Echtheit und der Quelle von Dokumenten.

Auditing: Lückenlose Sicherheitsüberprüfungen.

Vertraulichkeit wird bei Papyrus durch Verschlüsselung der Datenübertragung und aller gespeicherten Datenobjekte gesichert. Für Webanwendungen verwendet Papyrus HTTPS, das verschlüsselte Datenübertragungsprotokoll im Web. Es bietet authentifizierte und verschlüsselte Kommunikation für browserbasierten Zugang auf das WebPortal.

Autorisierung definiert die Funktionen, die eine identifizierte Person in einer Anwendung oder Systemressource ausführen darf. Dies wird durch Zuordnung zu einer bestimmten Benutzergruppe gewährleistet, ähnlich wie ein Theaterbesucher die Einrittskarte vorzuweisen hat. Das integrierte Autorisierungssystem garantiert, daß nur definierte Benutzer und Programme auf das System zugreifen können.

Im Projekt wird die Organisationsstruktur Ihres Unternehmens in Rollen und Berechtigungsgruppen definiert und diese dann Mitarbeitern zugeordnet.



Der Benutzer kann zum Beispiel berechtigt sein, eine bestimmte Funktion für einen bestimmten Brieftyp auszuführen. Diese Berechtigung kann gleichzeitig auch auf den Zugriff auf diesen Brieftyp für eine bestimmte Abteilung beschränkt sein. Der Papyrus LDAP-Adapter ermöglicht die Verwendung von bestehenden LDAP Benutzerrollen wie etwa aus RACF oder Active Directory.

Nachverfolgung und Zurechenbarkeit wird durch Kombination von Benutzerautorisierung und Auditfunktionen für Workflows erreicht. Da jeder Benutzer durch SmartCard und Fingerabdruck eindeutig identifiziert ist, und er einer ROLLE bzw. POLICY mit entsprechenden Zugriffsrechten zugeordnet ist, können sämtliche Aktivitäten des Benutzers in einem Audit Log protokolliert werden. Dementsprechend kann jede Aktivität einer dafür verantwortlichen Person garantiert zugeordnet werden.

Dies ist vor allem für System-, Sicherheits-, Change-Management Administratoren, Produktionsmanager oder für Anwender mit Freigaberechten von großer Wichtigkeit.

Authentizität: Sobald ein Dokument unternehmensweit verfügbar wird oder in öffentlich zugänglichen Umgebungen wie einer Website verwendet wird, kann der Dokumentenstatus auf ORIGINAL gesetzt werden. Das Dokument wird dann verschlüsselt und digital signiert. Dadurch kann das Dokument nur noch von autorisierten Benutzern geöffnet werden. Solange die digitale Signatur intakt ist, steht die Authentizität des Dokuments eindeutig fest, und das Dokument muß nicht auf Write-Only Medien gespeichert werden. Außerdem kann ein Dokument von Benutzern nur dann gelesen werden, wenn diese über den entsprechenden Private Key verfügen.

Auditing Analysebericht

Auditing wird durch das Nachverfolgen von Benutzeraktivitäten entsprechend festgelegter Regeln erzielt. Nur autorisierte Benutzer können dann erfasste Audit-Informationen auswerten und prüfen. Auditing wird auch zur Prüfung von Veränderungen in Sicherheitsdefinitionen benutzt. Es kann auch dazu verwendet werden, um den Weg eines Dokuments durch das Unternehmen nachzuverfolgen. Dazu werden dann auch Sicherheitsfunktionen wie Authentifizierung und Logging herangezogen.

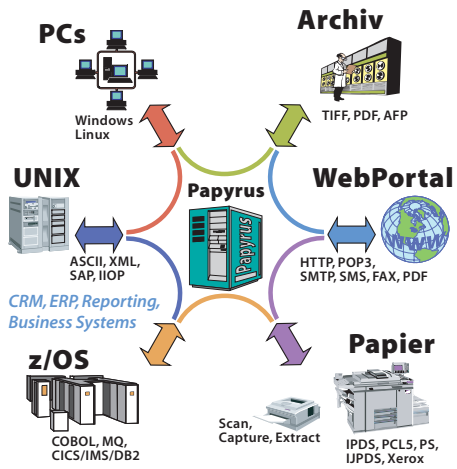
Motivation *für* INNOVATION

Motivation: Einhaltung von Datenschutz- und Archivierungsvorschriften

Innovation: Integration von SmartCard Authentifizierung in ein ECM System

Solution: Sicherheitsfunktionen des Papyrus Document Switchboards

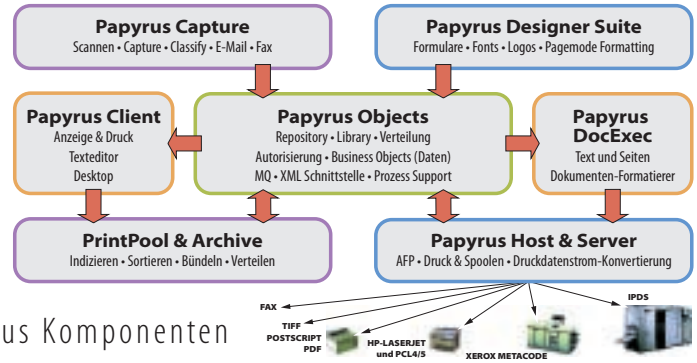
Eine **umfassende und skalierbare Lösung** für das Zentrale Management von Dokumentenanwendungen, Druck und Output Management, welche Web, Client/Server und Host Umgebungen einschließt.



Papyrus Document Frameworks

- Automated Document Factory
- Enterprise Application Integration
- Enterprise Output Management
- Enterprise Content Management
- Business Process Management
- Portal- und Webapplikationen
- Change Management
- Korrespondenz
- Campaign Management
- Print Management
- Capture/Klassifizieren/Extrahieren
- E-Mail/Fax

Organisationen **definieren, messen und verwalten** den Output über komplexe heterogene Umgebungen hinweg von zentralen Kontrollpunkten.



Papyrus Komponenten

Eine Auswahl aus den über 2000 ISIS Papyrus Referenzen:

Bankwesen arbeitet mit Papyrus

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

Versicherungswesen arbeitet mit Papyrus

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

Gesundheitswesen arbeitet mit Papyrus

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

Telekommunikation arbeitet mit Papyrus

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

Öffentliche Verwaltung arbeitet mit Papyrus

Commonwealth of Pennsylvenia, Europäisches Patentamt, Stadt Düsseldorf

Industrie arbeitet mit Papyrus

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

ISIS Lokationen

Internationale Zentrale, Österreich

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

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

Amerika Zentrale

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

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

Asien Zentrale

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

Deutschland

ISIS Papyrus Deutschland GmbH
Heerdter Lohweg 81
D-40549 Düsseldorf

T: +43-2236-27551
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

Italien

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

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

Frankreich

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

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

Spanien

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