



- ✓ Authenticity
- ✓ Reliability
- ✓ Integrity
- ✓ Tracking

#### Compliant with the standards:

ISO 14 721  
Open Archival Information System  
ISO 15 489-1  
Records Management  
ISO 19 005-1  
Use of the PDF format for filing (PDF/A-1)  
MoREQ:  
Model Requirements for the Management of Electronic Records

#### Compliant with the statutory and regulatory requirements

- Directive 2004/39/CE MiFID
- Directive 1999/93/EC on a Community Framework for Electronic Signatures, plus national\* regulations
- Directive 95/46/EC on the Protection of Personal Data, plus national\* regulations
- Basle II, Gramm-Leach-Bliley Act, Sarbanes-Oxley, COSO (Switzerland) plus national\* financial sector regulations
- SAFE, HIPPA and national\* health sector regulations

\* WIS@key SA recommends that you examine the laws of your country

## WIS@MiFID

**The Markets in Financial Instruments Directive (MiFID) is already trumpeted as the biggest change to happen in financial services.**

It is important for financial institutions to have a good understanding of what is needed to achieve the information system requirements and to have the right solution to attain the goal.

WIS@Key has assessed the impact of MiFID in the financial services marketplace and offers technologies like CertifyID BlackBox™ on what steps financial services companies can take to prepare for these significant changes.

### E-mail compliance MiFID with CertifyID BlackBox™

In the Microsoft Exchange Server 2007 architecture journaling is enabled at the mailbox store level. The reason you cannot forward journalized messages directly from the mailbox database where journaling is enabled is because some of the envelope data (for example, Bcc recipients and expanded distribution list recipients) is added by the Exchange Information Store service upon delivery to the journaling mailbox. Therefore, if you journal all mail directly to SMTP, Bcc and expanded distribution list recipient data is lost, but WIS@Key has the solution integrated : CertifyID BlackBox™.

**The decentralisation of the authority of certification CertifyID BlackBox™ allows avoiding these risks.**

### Records Management Requirements on MiFID

Records are created, received and used in the conduct of business activities. To support the continuing conduct of business, comply with the MiFID regulatory environment, and provide necessary accountability, organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required. To do this, organizations should institute and carry out a comprehensive records management programme which includes CertifyID BlackBox™ from WIS@Key.

### Authenticity

To ensure the authenticity of records, organizations should implement WIS@Key Solutions which controls the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment.

### Reliability

To ensure the reliability of records, organizations should implement WIS@Key Solutions. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

### Integrity

To ensure the integrity of records, organizations should implement WIS@Key Solutions.

It is necessary that a record be protected against unauthorized alteration. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

### Tracking

Tracking of the movement and use of records within a records system required WIS@Key Solutions.

For more information, please visit:  
[www.wisekey.com](http://www.wisekey.com)