



# KYC and MiFID **SHARED OPPORTUNITIES**

White Paper  
November 2006

# Table of Contents

New Regulations in European Banking ..... 3

Summary of Legislative Requirements ..... 4

KYC ..... 4

MiFID ..... 4

Client Management Process ..... 6

Suggested Approach ..... 7

Summary ..... 9

## Chapter 1

# New Regulations in European Banking

There are similarities between MiFID and KYC that banks should look at for potential cost savings and client service advantages from having a shared approach to the two regulations.

The European banking industry is being faced with huge regulatory burden at the moment, which is necessitating significant investment in new processes and accompanying IT. In particular MiFID will reshape the wholesale and investment banking landscape and how they inter-react with the buy-side and private clients. In the long term this will cause greater competition throughout Europe through more liquidity pools and greater transparency. It will also increase investor protection particularly for high net worth individuals.

The implementation of MiFID is expected to increase access to capital, and improve the efficiency of European capital markets to the extent of adding a full 1% to ongoing European economic growth<sup>1</sup>. All this is not without cost and whilst estimates of the required investments vary, it is unlikely to be less than 1Bn Euros being borne by the industry<sup>2</sup>. It is also expected that those that make the investments will be playing in a much more competitive market to the extent that analysts have recently down graded many investment bank stocks due to expected reductions in earnings per share<sup>3</sup>. This reduction is greatest for those that have an integrated banking model between private clients and the in-house investment bank.

The Know Your Customer regulations are also impacting the banks and especially the private client sections. Recent fines for AML compliance breaches have focussed the minds in some of the banks to increase the priority of compliance efforts.

Banks should investigate the areas of common impact on processes and systems to ensure that there is not duplication of effort and that those investments are made optimally.

Sun has already been working with its partners edge IPK, Mobius, and Morse on the KYC Alliance. This alliance is now being extended to cover the intersection of KYC and MiFID.

1. IT Analysis, Bob McDowell, IE4C

2. As noted by TowerGroup in report "Reg NMS & MiFID: A Tale of Two Regulations"

3. JP Morgan Chase see <http://www.finextra.com/fullstory.asp?id=15841>

## Chapter 2

# Summary of Legislative Requirements

## KYC

Know Your Customer (or KYC) presents a number of requirements when you take on a client and throughout the customer management lifecycle.

At client take-on the firm is required to:

- Verify the identity and address of the client by checking documentary evidence and performing external database searches and checks
- Perform a risk assessment including from an anti-money laundering perspective

Additionally a number of lifecycle reviews are required:

- Reviews are required triggered by events such as suspicious account behaviour as seen by an AML scanning engine or other techniques
- Periodic reviews of changes in client status and activity profiles

KYC also requires due care of records from a data protection and archival perspective.

## MiFID

The Markets in Financial Instruments Directive (MiFID) is extremely broad ranging. It is not the purpose of this short paper to look at the full scope of the directive's requirement but to just look at the overlap between it and KYC. Therefore we will discuss only those aspects of the directive that are relevant.

MiFID has a number of requirements on client take-on or at least initially as the directive goes live:

- Clients need to be classified as retail, professional or eligible counterparty
- The firm's best execution policy must be given to the client and his agreement gained
- The client must be profiled and if investment advice is to be given, then the firm must understand his financial knowledge and education, his attitude to risk and financial position to accept risk

On a periodic basis a firm is required to:

- Reassess the best execution policy and gain client agreement to any changes
- Reassess material changes to a clients situation

When providing execution based on investment advice a firm is required to:

- Assess whether a client has the skills and education to understand the risks associated with the product being recommended
- Ensure the product recommended is suitable for the financial needs of the client

MiFID also enables electronic communication with a client when the client agrees. This channel can then be used for the many responsibilities of client reporting. Apart from trade confirmations client reporting should also cover:

- The costs associated with the trade
- Any warnings given such that best execution could not be applied
- Whether the trade was executed OTC within the firm

From a records management perspective, MiFID requires client communications to be kept for five years. Also a client has the ability to query whether a trade followed the firm's best execution policy. To respond to this a firm should be able to recreate the full circumstances surrounding a trade, for all the products that best execution applies to (which is almost all). Not only would this normally require tick data and liquidity pool quotes to be stored, but also the details of the client interaction surrounding the trade. This could involve unstructured data such as telephone, voice and even instant message (IM) records, which could protect the firm by demonstrating a request, for example, to sell shares immediately outside the context of the normal best execution requirements. These records management requirements should ideally be augmented by advanced security that can be used in a court of law to assert the provenance of the data.

## Chapter 3

# The Client Management Process

All banks have some form of client management process. This would typically be split into a client take-on process and an ongoing management process which would contain an event driven and a periodic review process. This will be underpinned by a records management process.

Looking at the relevant MiFID requirements it can be seen that there is synergy between the process requirements of the two sets of legislation. Both have activities that need to happen:

- At client take-on
- On a periodic review process
- On an event (e.g. an AML trigger or a trade)
- For records management

If the firm does not integrate activities, for example, at client take-on then the client will be approached once for identity verification and then by a different group for profiling. If these two approaches can be integrated in one part of the bank with one set of systems, then not only will this appear more professional to the client but cost will be saved as one systems development will be undertaken with one set of software licenses for one team of client service staff.

Looking at a process level view of existing KYC processes, MiFID should add:

- For client take-on: client classification, profiling, re-papering and best execution policy agreement
- For periodic reviews to update the client profile for financial situation and risk appetite
- Event reviews are a feature of KYC. From a MiFID perspective a client interaction which involves investment advice requires the checking of suitability and appropriateness questions. These can be considered an event and recorded and archived as such. They might also be recorded in a customer service system.
- Exception events also need to be managed such as a client querying best execution on a particular trade. The query, its management and communications needs to be recorded.
- Depending on the scope of the KYC systems, client reporting can be addressed which include trade confirmations with the extended MiFID required information such as trade and settlement costs.

The creation of a single system for the shared aspects of KYC and MiFID across lines of business is not without its challenges. Some banks are organised not by product LoB but by geography. In this case integration of systems which may have unique data privacy laws demands close attention. An example might be Liechtenstein which does not allow personal data to leave its borders. This may drive a hybrid approach where data placement is key and complex rules based routing may be required to satisfy all demands.

Data integration will also be a key requirement for enabling a centralised approach. Such a strategy will need to overcome a number of key inhibitors:

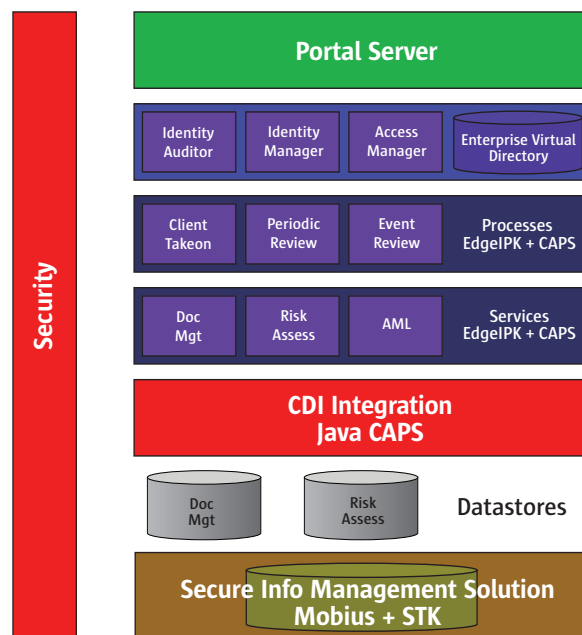
- It cannot be assumed that customer numbers are consistent in different lines of business for the same customer
- Existing KYC datastores may have similar data stored in different formats or with different interpretations
- It may not be possible either functionally or economically to scrap existing KYC datastores and merge them into one

## Chapter 4

## Suggested Approach

The high level requirements above can be summarised as follows:

- Rule based customer data integration across business units
- Consistent customer numbering across business units
- Flexibility to leave existing datastores untouched
- Archive capability that exploits existing datastores but also ideally adds evidential integrity to the storage of those records plus the ability to recreate the circumstances of a trade including voice, email and IM
- A flexible and productive forms generation and business process automation environment, ideally based on SOA technologies, that can be used to create form based process-driven applications
- Strong identity management to enforce and audit staff access rules to client data. Ideally this should also be able to provision external client identities for such applications as access to client communications and reports or trade analysis and status.



This architecture combines the technologies of three market leading companies: edge IPK, Mobius and Sun Microsystems with the systems integration skills of Morse, enabling an integrated solution that meets all the challenging requirements above.

At its core is the Secure Information Management Solution (SIMS) from Mobius and Sun. This is an enterprise archive with a number of special features that make it suitable for the needs discussed here, including:

- Use of cryptographic enabled tape drives for data protection
- Use of WORM tape for secure audit logging
- Optional sealing technologies for evidential integrity
- Content integration software that gives a single customer view across multiple datastores
- Migration technologies that allow for data to reside in existing datastores or be moved into a central archive

Mobius provides a highly scalable archiving solution that can scale beyond terabytes of information – the world’s largest archive is currently managed by Mobius and is in excess of 18 petabytes! The software applies retention and disposition rules to the information and also includes extensive indexing for accurate and fast search performance. Content integration software from Mobius provides fast, easy, and secure access to all content stored anywhere in the enterprise. It integrates client information into one virtual archive and gives authorised users a single, consistent interface to multiple, disparate content sources. Mobius is certified to run on Sun’s industry leading range of storage products that include fast access fibre channel disk, lower cost NAS products and tape.

The Sun Identity Management Suite is the world’s leading enterprise scale identity platform providing user identity provisioning, application access management and auditing plus massive scalability for an enterprise user directory. It also allows the mapping of an enterprise identity to its existing in-place line of business equivalent identities.

The Sun Composite Application Platform Suite (CAPS), is a leading messaging and SOA based integration layer that easily wrap legacy applications and expose them as SOA services, as well as using heuristic rules to resolve discrepancies between conflicting data fields from differing data sources to contribute to that single customer view. This software is in use in the worlds largest integration project at a major european healthcare provider.

edge IPK provides a powerful massively productive environment for the development and running of browser based applications that have the flexibility to be deployed as fat or thin client, off-line, in a Portal or Application Server.

edgeKYC provides a single solution that allows you to standardise KYC processes across the enterprise whilst providing flexibility for local country regulatory requirements. Each jurisdiction can therefore follow a consistent way of working, regardless of location, language and business function/business role. Whilst enabling regulations for each jurisdiction to be seamlessly integrated into the system to ensure compliance with local and international guidelines.

edgeKYC is executed on the edgeConnect platform which provides a powerful massively productive environment for the customisation and execution of browser based applications that have the flexibility to be deployed as Rich, Thin Portal or Off-line applications. edgeConnect provides the performance, scalability and security that is required to automate KYC and MiFID business processes for an entire global enterprise.

Morse delivers the consulting, technology and support services around the KYC Alliance platform that enables organisational change, improved efficiency and greater value from this investment. With its breadth and depth of expertise and long experience of working closely with Europe’s Tier 1 financial institutions, Morse can help them evolve their strategies and solutions to align with the requirements of KYC and MiFID. Consultants from the Morse Enterprise Content Management practice have vast experience in helping financial services organisations develop and implement information management strategies to control the increasing amounts of unstructured corporate information that is subject to ever greater scrutiny by shareholders, clients, internal auditors and external regulators.

## Chapter 5

# Summary

Firms that offer investment advice have significant requirements from both KYC and MiFID, and should look carefully at how they can structure to take advantage of process overlaps in the way they interact with clients.

The KYC Alliance of edgeIPK, Mobius, Morse and Sun Microsystems already have experience in working together in major financial institutions on KYC, and have done significant work in assessing the opportunities to apply this same proven technology base into MiFID client lifecycle management requirements. By with you, we can take advantage of best of breed products in a way that is designed to decrease overall cost and improve client service whilst reducing implementation risk.

For more information please contact [KYC-Alliance@sun.com](mailto:KYC-Alliance@sun.com)

© 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, and the Sun logo are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.

**MORSE**



**Sun Microsystems, Inc.** 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com

©2006 Sun Microsystems, Inc. All right reserved Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.