TMF Group
Project SEO.NEXT

Concept paper

Version 1.0
16.12.2013

Content

Tables

Figures

1 Initial position and objectives

The objective of this paper is to give an in-depth view on the current status of SEO and the requirements for the future application for TMF Compliance, herein called SEO.NEXT as project name.

The whole concept includes more than this document. References to spreadsheets, screenshots, process graphics etc. are used. Those resources are an integral part of the concept and have to be used for the full understanding of it.

This concept follows the agile principles and will change during the construction phase of the project as new and changed requirements will inevitably occur.

2 Glossary

The glossary helps to have the same understanding of terms used in the application and the project. Therefore it is important to add any term which is capable of being misunderstood or ambiguous during the project for future reference.

ID	Term / Label	Abbr	SEO.OLD	Context	Description
01	Client		-		Individual or legal person related to a mandate
02	Mandate		-		Client entity, TMFs' business relation
03	Ultimate Beneficial Owner	UBO	-	Obj/Links	For AML-relevant mandates: "Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
04	Ultimate Beneficial Owner Light	UBL	-	Obj/Links	
05	Preliminary Intake Approval	PIA	-	Document	
06	Client Acceptance Form	CAF	-	Document	
07	Basic Doc / Basic Documentation	-	GRUDO	Client / Mandate	Client or Mandate profile document/record
08	Basic Doc 1	-	GRUDO I	Client	Client profile
09	Basic Doc 2	-	GRUDO II	Mandate	Mandate profile
10	Group Compliance Officer	GCO	-	Process	Compliance Officer responsible for TMF group
11	Local Compliance Officer	LCO	-	Process	Compliance Officer responsible for TMF's office
12	Account Manager	AM	Mandate Manager	Process	Client Entity Manager in direct contact with the clients
13	System under Development	SuD	-	Architecture	Technical name of SEO.NEXT
14	Risk profile	-	Rima file	Risk management	Risk assessment profile of each mandate available in SEO

Table 1: Glossary

3 Application Overview

3.1 Intention of the application

The intention of the application is to manage all information about clients and mandates of the TMF Group relevant to the duties of Group Compliance.

3.2 Application Platform

3.2.1 Server Components

- Microsoft Windows Server 2003 SP3 32-bit
- IBM Lotus Domino Server 8.5.1 FP3 English 32-bit
- Gupta SQLBase Server 8.5.1
- IBM Lotus NotesSQL 8.0
- Crystal Report Application Server 9.0

3.2.2 SEO Compliance Modules (Application Templates and databases)

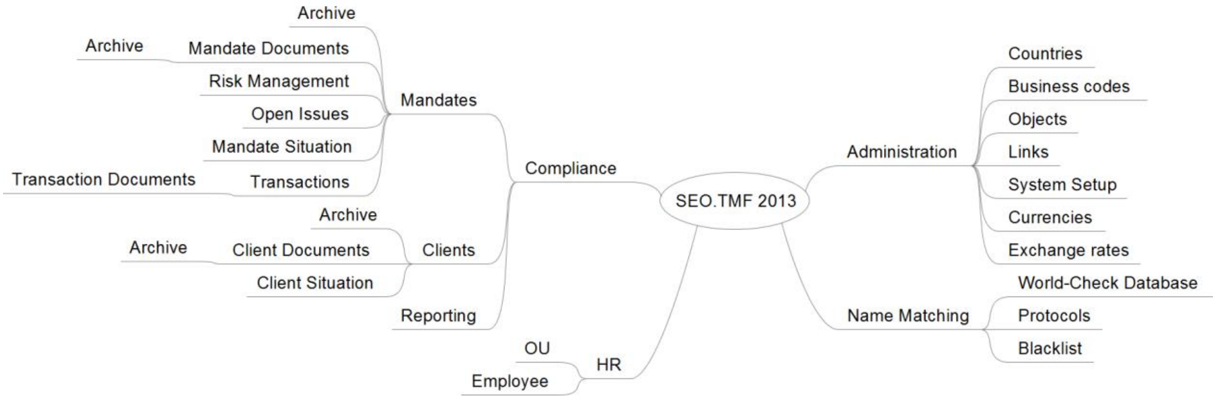


Figure 1: SEO Compliance Modules

Key	Name	Module	Description
GRDI	Grudo I (KYC Client)	Compliance	Client data (individual/legal) Management (BasicDoc1)
GRDII	Grudo II (KYC Mandate)	Compliance	Mandate data Management (BasicDoc2)
ARCGRDI	Grudo I Archive (KYC Client Archive)	Compliance	Archive database for client data
ARCGRDII	Grudo II Archive (KYC Mandate Archive)	Compliance	Archive database for mandate data
TASK	Open Issues	Compliance	Open issues of a mandate
TRANS	Transactions	Compliance	Transaction documentation to mandates
RISK	Risk Management	Compliance	Risk rating for mandates
CS	Client situation	Compliance	
MS	Mandate situation	Compliance	

DMC	Document Management Client	Compliance	
DMM	Document Management Mandate	Compliance	
DMT	Document Management Transaction	Compliance	
ARCDMC	Document Management Client Archive	Compliance	
ARCDMM	Document Management Mandate Archive	Compliance	
HM	Hit management	Compliance	
NM	World-Check Database	Name Matching	
NMP	Name Matching Protocols	Name Matching	
BL	Blacklist	Name Matching	
PRS	Employee	Human Resources	
OU	OU	Human Resources	
BRA	Business codes	Administration	
CTY	Countries	Administration	
CUR	Currencies	Administration	
FX	Exchange rates	Administration	
LINK	Links	Administration	
OBJ	Objects	Administration	
SYS	System setup	Administration	

Table 2: SEO Compliance Applications

This list only includes modules effectively used by TMF.

3.3 Future Software Platform

- Microsoft Windows Server 2008 R2 or 2012 R2
- Microsoft SharePoint 2013 or SharePoint 2013 SP1
- Microsoft SQLServer 2008 R2 or 2012 R2 Standard/Enterprise Edition

Note: More information in section 8.3

3.4 Stakeholders and Actors

Table of the applications stakeholders and actors and their possible concerns and attitude in relation to the application.

Key	Stakeholder	Role	Benefits	Concerns	Att.
CEO	Chief Executive Officer	Final responsible, approves information	Minimize reputation risk	Administration overhead	+
LEG	Legal department	Approves information	Avoid legal issues	-	0
GCO	Group Compliance Office	Manages, reviews and approves information Responsible for processes	Control		++
LCO	Local Compliance Office	Approves information	Control	Administration overhead	+

AM	Account Manager	Delivers information	active reinsurance Single point of information	Grand effort Client rejection	-
CL	Client		?	Slows down process	-
ITM	IT-Management	Responsible for development and operation of application		Administration overhead, limited knowledge	0
ITS	IT-System Administrator	Operator and administrator	?	Not enough control, limited access	-

Table 3: Stakeholders and actors

3.5 Access rights levels and User Roles model

Basic functions: S=Search; C=Create; R=Read; U=Update; D=Delete

	Role	Name	Scope (Access)	Basic functions	Modules	Status
Group Level	**MGT**	Management	Global except administration	SR	Compliance, Name Matching	Active
	GCOp	Group Compliance privileged	Global except administration	SCRU(D)	Compliance, Name Matching, Administration	New
	GCO	Group Compliance	Global except administration	SCRU	Compliance, Name Matching	Active
Office Level	**LMGT**	Local Management	Public or assigned to their office(s)	R	Compliance, Name Matching	New
	LCO	Local Compliance	Public or assigned to their office(s)	CRU	Compliance, Name Matching	Active
	AM	Account Manager	Public or assigned to their team(s) or themselves	R	Compliance, Name Matching	Active
System Level	**AA**	Application Administrator	Application administration only, no data	-	Administration	Active
	SA	System Administrator	System administration, monitoring maintenance	-	-	New

Table 4: User roles

3.5.1 Office and Team Structures

Offices are an important organizational unit within TMF Compliance. It is a central hub for relating clients and mandates to employees. The new unit level “Team” breaks down the hierarchy on the next level, grouping employees of one office to a team.

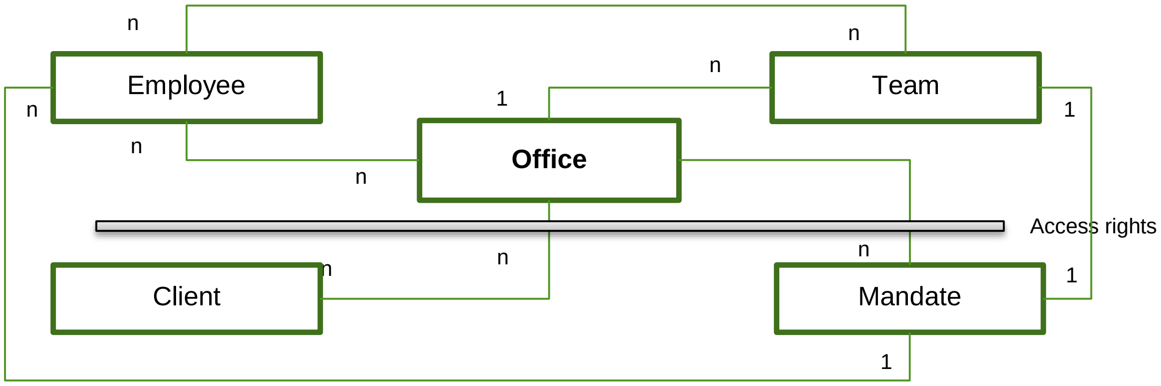


Figure 2: Office and Teams

Also in terms of access level rights, this structure is important for the roles of “Office Level”.

- Local Compliance and Local Management only have access to their clients and mandate of their office.
- Account Managers only have access to mandates of their office, if they are either named as Account Manager/Contact on the mandate or part of the team the mandate is assigned to.
- LMGT, LCO, and AM can be assigned to more than one office and team
- Offices can have more than one LMGT, LCO, and AM
- Clients have zero to many offices assigned
- Clients without office assignment are public (to application users)
- Mandates have one primary Account Manager
- Mandates have zero to many additional contacts (assigned employees)
- Mandates have zero to one team assigned

3.5.2 Application rights for roles

See table in file “TMF-SEO.NEXT-RoleModel_final.xlsx” (currently in revision – no final version available yet)

3.6 Objects and Links

SEO uses so called objects with their object definition and link definitions to link objects in a certain way. Currently the following definition are available. Only active links and objects have to be created.

3.6.1 Link definitions

ID	Short	Name	Status
L01	UBO	Ultimate Beneficial Owner	A
L02	BE	Beneficiary	A
L03	LB	Ultimate Beneficial Owner Light (UBL)	A
L04	SE	Settlor	A
L05	DI	Director	A
L06	FM	Other relations	A
Technical links for Name Matching Profiles, which are not set and maintained by the user himself, but created by the system (informational only, no need to be implemented in SuD)			
L07	NM_PRSPROT	NameMatching Person Search Protocol	A
L08	NM_SEOPROT	NameMatching SEO Check Protocol	I

L09	NM_WCPROT	Name Matching World-Check Profile	A
L10	NM_WC_PRS	NameMatching World-Check Person Protocol	A
World-Check links, which are not set and maintained by the user himself, but created by the system. Links must be available, based on World-Check XML structure.			
L11	WC_LINKED_TO	Worldcheck Linked to	A
L12	WC_LINKED_TO_C	Worldcheck Linked to (Company)	A
L13	WC_COMPANY_LINKED	Worldcheck Company Linked	A

Table 5: Link definitions

3.6.2 Object definitions

ID	Short	Name	Rel. Modules	Status
O01	GRDIIL	AML Mandate	GRDII ARCGRDII	A
O02	GRDIIS	Non AML Mandate	GRDII ARCGRDII	A
O03	GRD1BOIND	UBO / Beneficiary / Settlor Individual	GRDI ARCGRDI	A
O04	GRD1BOLEG	UBO / Beneficiary / Settlor Legal	GRDI ARCGRDI	A
O05	GRD1LBIND	UBO Light / Director Individual	GRDI ARCGRDI	A
O06	GRD1LBLEG	UBO Light / Director Legal	GRDI ARCGRDI	A
O07	TRANSACTION	Transaction	TRANS	A
O08	CA QU AOA FA MA CoC RoD RoM TD 1560 BVI PPM REC 1570 COR OAD OTH	Client Acceptance Questionnaire Articles of Association Financial Statements Service/Management Agreement Excerpt Chamber of Commerce Register of Directors Register of Members Trust Documents Form A Tax Advice PPM Certificate of Recognition Structure Chart Correspondence Other Agreements/Deeds Other	DMC DMM DMT ARCDMC ARCDMM	A
O09	WorldCheck	World-Check Profile	NM	A
O10	TMFBLACK	TMF Blacklisted Persons	NM	A
O11	NameMatch_Search_PRS	NameMatch Client-Searchprotocol	NMP	A
O12	NameMatch_Search_SEO	NameMatch SEO - Checkprotocol	NMP	I
O13	NameMatch_File_WorldCheck	NameMatch File - WorldCheck	NMP	A

Table 6: Objects definitions

3.6.3 Object-links matching table

Objects													
	O01	O02	O03	O04	O05	O06	O07	O08	O09	O10	O11	O12	O13
O01	*New*	*New*	L01 L02 L04 L05 L06	L01 L02 L04 L05 L06	-	-	-	-	-	-	-	L08	L09 L10
O02	*New*	*New*	L03 L05 L06	L03 L05 L06	L03 L05 L06	L03 L05 L06	-	-	-	-	-	L08	L09 L10
O03	L01 L02 L04 L05 L06	L03 L05 L06	New	New	New	New	-	-	-	-	L07	L07 L08	L07 L09 L10
O04	L01 L02 L04 L05 L06	L03 L05 L06	New	New	New	New	-	-	-	-	L07	L07 L08	L07 L09 L10
O05	-	L03 L05 L06	New	New	New	New	-	-	-	-	L07	L07 L08	L07 L09 L10
O06	-	L03 L05 L06	New	New	New	New	-	-	-	-	L07	L07 L08	L07 L09 L10
O07	-	-	-	-	-	-	-	-	-	-	L07	-	L09
O08	-	-	-	-	-	-	-	-	-	-	-	-	-
O09	-	-	-	-	-	-	-	-	L11 L12 L13	-	-	-	-
O10	-	-	-	-	-	-	-	-	-	-	-	-	-
O11	L07	L07	L07	L07	L07	L07	L07	-	-	-	-	-	-
O12	L08	L08	L07 L08	L07 L08	L07 L08	L07 L08	-	-	-	-	-	-	-
O13	L09 L10	L09 L10	L07 L09 L10	L07 L09 L10	L07 L09 L10	L07 L09 L10	L09	-	-	-	-	-	-

Table 7: Object-links matching table

3.7 Field definitions

See tables in files
“TMF-SEO.NEXT-Fieldlist_final.xlsx” and
“TMF-SEO.NEXT-FieldList_Administrative_final.xlsx”

4 Processes

Note: All process diagrams are available as PNG graphics (additional resources).

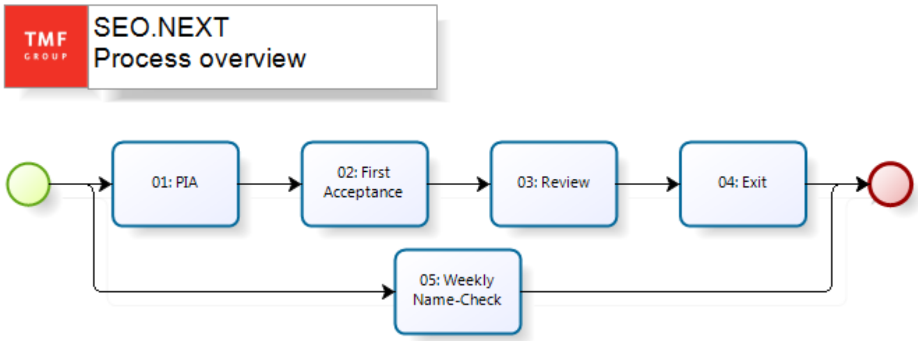


Figure 3: Process overview

4.1 Preliminary Intake Approval (PIA)

Customer-interaction at TMF Compliance starts with the Preliminary Intake Approval process. Objective of this process is to validate initial, basic informations of a likely future client or business relation in order to allow account managers further negotiations with their client without major risks for TMF. The process starts with the delivery of the standardized document “Compliance Questionnaire”, signed by the customer and ends usually with the standardized document “Group Compliance – Preliminary Intake Approval” signed by GCO Brunnen. Exceptionally the process ends if a client is rejected by the Group Compliance Officer.

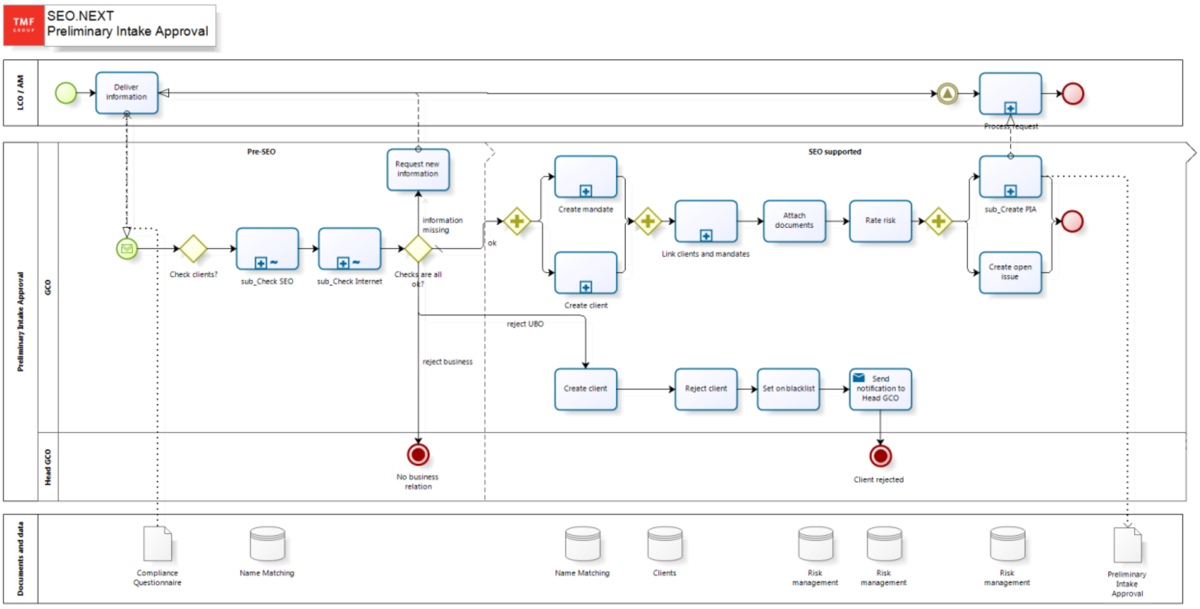


Figure 4: Process diagram PIA

The process also includes three sub processes which are shown consecutively:

Sub Process "Check SEO"

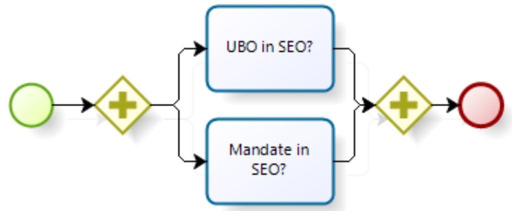


Figure 5: Sub process diagram Check SEO

Sub Process "Check Internet"

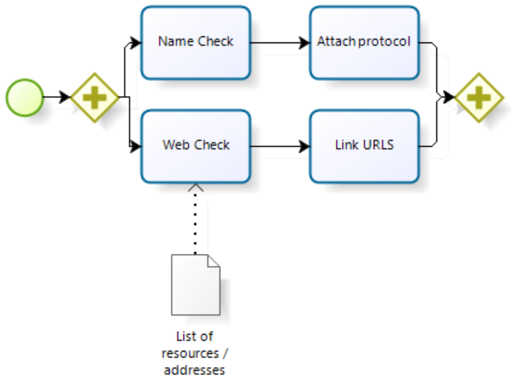


Figure 6: Sub process diagram Check Internet

Sub Process "Create PIA"

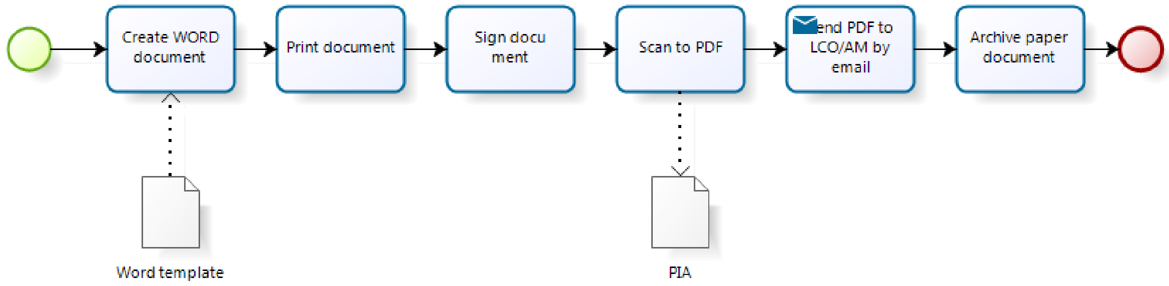


Figure 7: Sub process diagram Create PIA

4.2 First Acceptance

After the Preliminary Intake Approval has been processed and the document has been archived, the process First Acceptance starts, waiting for the requested documents to be delivered.
Once they arrive at Group Compliance, the documents are processed and data entered into the TMF Compliance System. The objective of the process is to finally accept the customer and official start the business relation.
Acceptance of any customer is done by the CEO and is a paper-based process. All documents and information is archived and managed in TMF Compliance System.

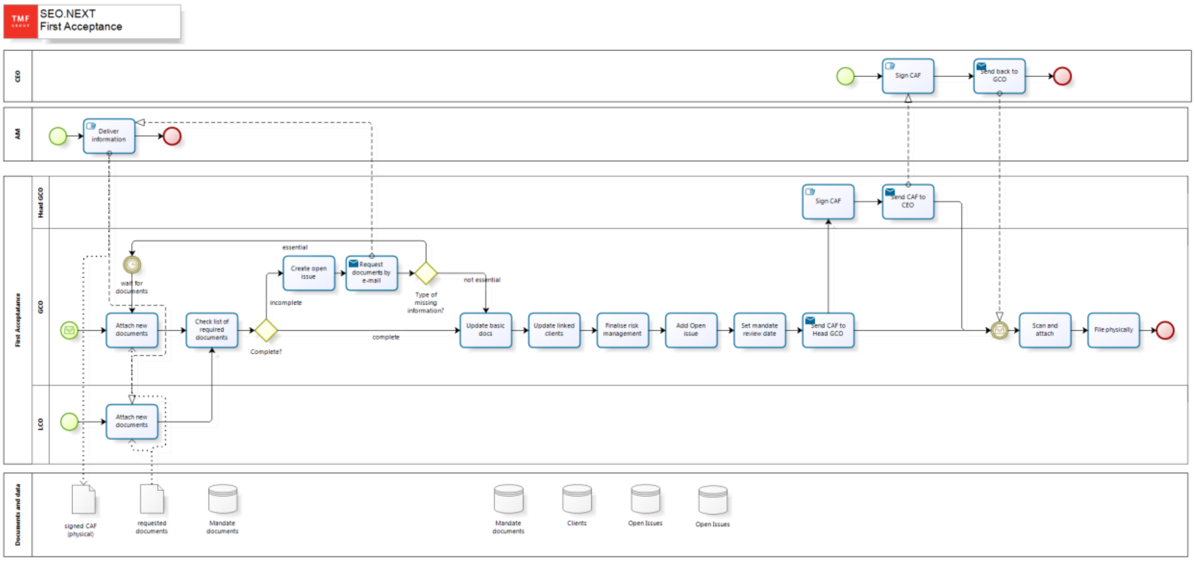


Figure 8: Process diagram First Acceptance

4.3 Review

The review process basically covers the same activities as the First Acceptance process with slightly different roles involved. It is processed as periodical check to review the existing business relation and the accuracy of the available data. The review also is documented in the system, amendments of client and mandate data results in versioning of basic documentations.

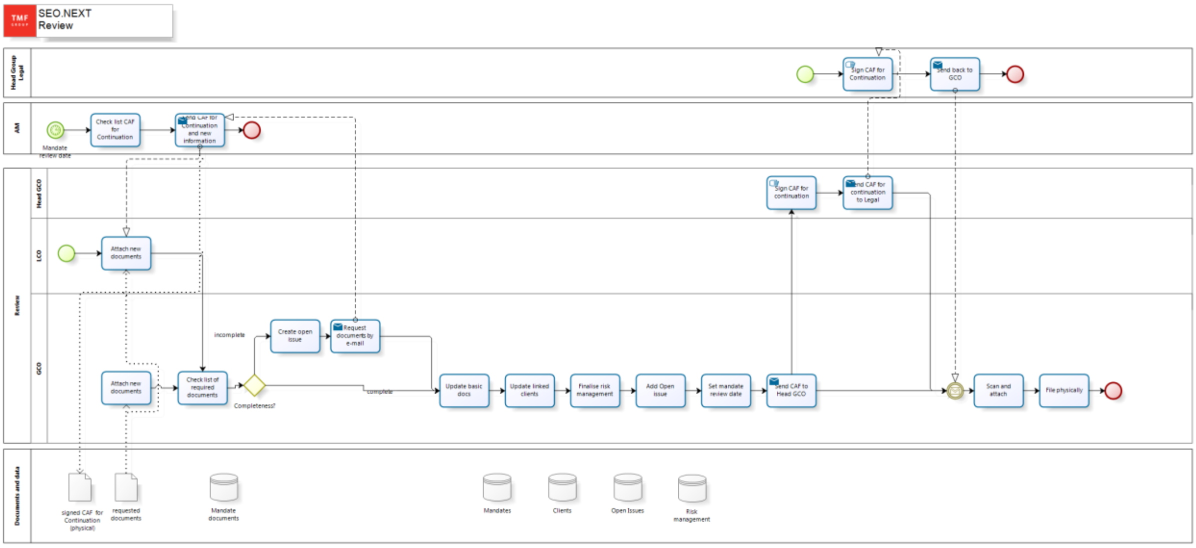


Figure 9: Process diagram Review

4.4 Weekly Name-Check

The weekly name-check process describes in general a task, group compliance team performs periodically, today on a weekly basis. The process consists of automated system tasks – import World-Check XML data and process the name matching check – as well as of human tasks to rate and comment the hits.

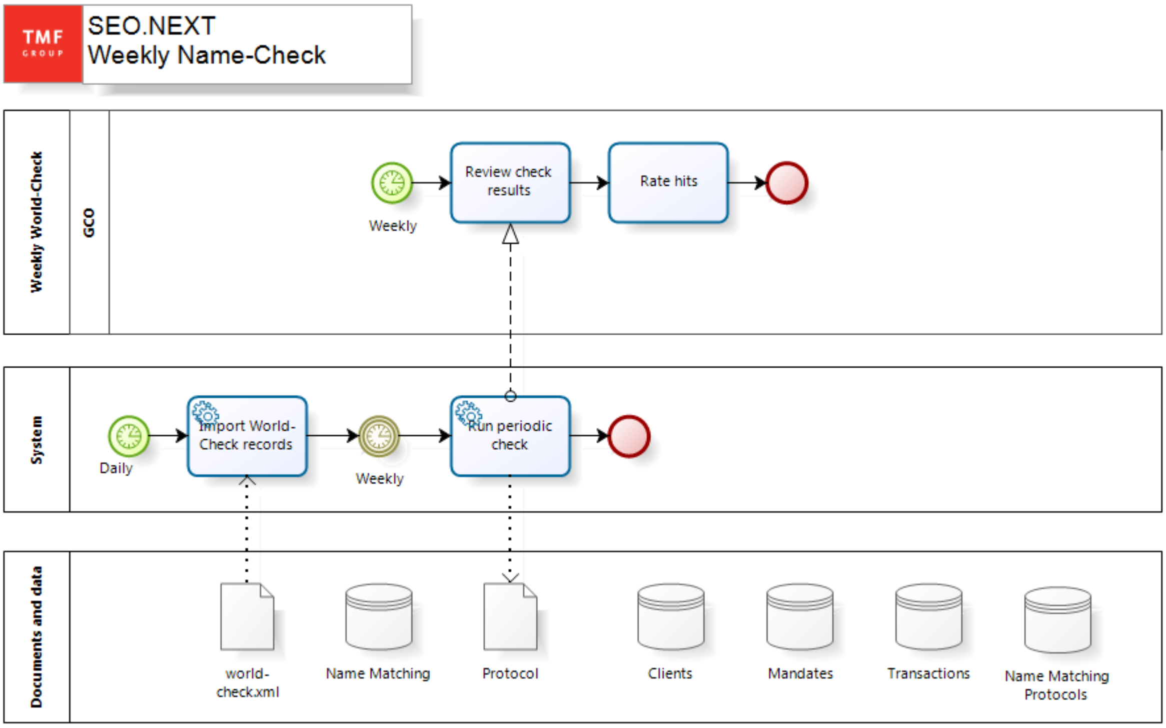


Figure 10: Process diagram Weekly Name-Check

The name matching check itself compares the names available in TMF Compliance databases (clients, mandates, transactions) with the names available in World-Check and TMF Blacklist databases.

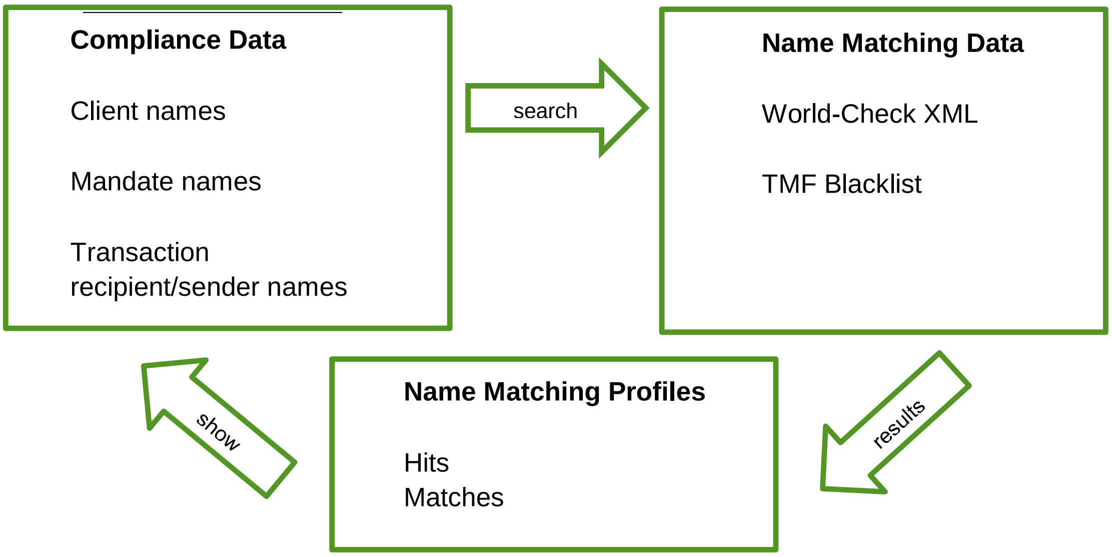


Figure 11: Name-Check

4.5 Exit

The exit process describes the actions taken in the Compliance system once a business relation has been terminated. The process starts with the incoming exit sheet and proof of exit and ends when all clients' links and mandates involved are inactive and the mandate situation has been updated. Client remain active if other links to active mandates exist.

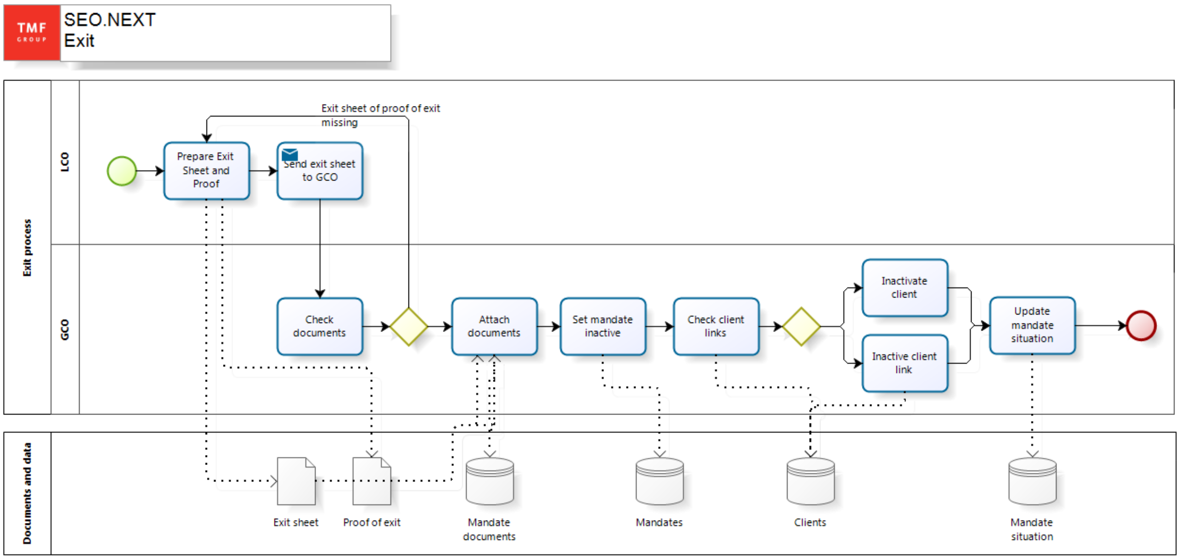


Figure 12: Process diagram Exit

Business Requirements

5 Epics and Themes

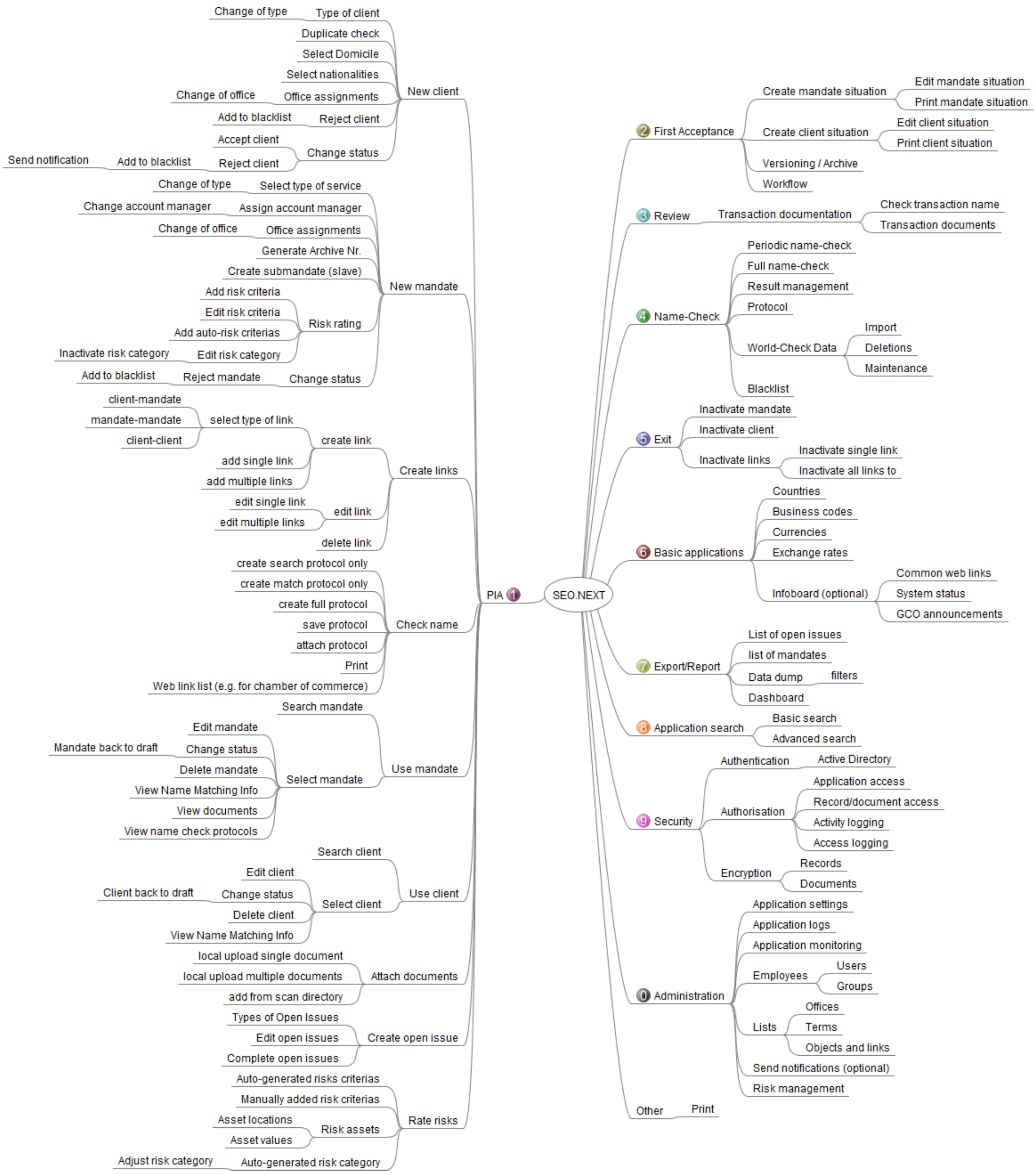


Figure 13: Overview Epics

Epics are larger scenarios or themes which group several single user stories to a major objective within the application. They are used here to give an overview and group functional aspects of the application and assign them to the processes. If an epics is assigned to a process this doesn’t mean that it is only available in this context. Usually this only refers to the process where this epic first occurs.

5.1 Preliminary Intake Approval (PIA)

Epic New client	
Number	EPIC-001
Group	PIA
Theme	Client
Parent epic	-
Description	As compliance officer I want to create a new client, either as a legal or an individual person, based on the information of the Compliance Questionnaire.
Resources	Figure 23: Create client individual Figure 24: Create client legal File: Compliance Questionnaire 08_2012 Form
Comments	The data set of individual and legal persons differ slightly. Please see also the data model and field list spreadsheets.

Table 8: Epic New client

Epic New mandate	
Number	EPIC-002
Group	PIA
Theme	Mandate
Parent epic	-
Description	As compliance officer I want to create a new mandate based on the information of the Compliance Questionnaire.
Resources	Figure 25: Create mandate File: Compliance Questionnaire 08_2012 Form
Comments	Services provided to the customer force the profile type of the mandate. The link requirements for AML relevant mandates and NON AML relevant mandates differ slightly.

Table 9: Epic New mandate

Epic Create links	
Number	EPIC-003
Group	PIA
Theme	Links
Parent epic	-
Description	As compliance officer I want to create links between different entities like clients and mandates in order to visualize and manage all relations.
Resources	Chapter 3.6.1 Figure 26: Create links
Comments	

Table 10: Epic Create link

Epic Check name	
Number	EPIC-004
Group	PIA
Theme	Name Check
Parent epic	-
Description	As compliance officer I want to check the names of clients and mandates by using the

	integrated name matching database in order to verify and document the current status of the client or mandate.
Resources	-
Comments	Use Name Matching database with World-Check and TMF Blacklist data. Optional: Web-resources integration

Table 11: Epic Check name

Epic Use client	
Number	EPIC-005
Group	PIA
Theme	Client
Parent epic	-
Description	As a local compliance officer or group level user I want to look up a client and view or edit the information according to my access level.
Resources	Figure 27: Select client Figure 28: Basic doc client individual - profile tab Figure 29: Basic doc client individual - professional background tab
Comments	Includes client search and basic documentation actions.

Table 12: Epic Use client

Epic Use mandate	
Number	EPIC-006
Group	PIA
Theme	Mandate
Parent epic	-
Description	As an office or group level user I want to look up a mandate and view or edit the information according to my access level.
Resources	Figure 30: Basic doc mandate - profile tab Figure 31: Basic doc mandate - business activities tab
Comments	Includes mandate search and basic documentation actions.

Table 13: Epic Use mandate

Epic Attach documents	
Number	EPIC-007
Group	PIA
Theme	Document
Parent epic	-
Description	As a local or group compliance officer I want to attach (upload) single or multiple electronic documents related to a client or a mandate.
Resources	-
Comments	Supporting all file types, but mainly PDF are used.

Table 14: Epic Attach documents

Epic Risk rating	
Number	EPIC-028
Group	PIA
Theme	Risk management
Parent epic	-

Description	As a group compliance officer I want to manage the mandates' risk by assigning risk criterias in order to classify the mandate with a risk category.
Resources	Figure 38: Risk profile
Comments	Risk profile consists of risk criteria, risk asset values and risk asset locations resulting in a risk category.

Table 15: Epic Risk rating

Epic Create open issue	
Number	EPIC-008
Group	PIA
Theme	Open Issue
Parent epic	-
Description	As a group compliance officer I want to create open issues to a mandate in order to track and manage to-dos of account managers, local and group compliance officers.
Resources	Figure 32: Create open issue - type basic doc
Comments	Open Issues are like tasks – Task management component in SEO. Tasks are never assigned to people or groups, only to mandates. Employees responsible for the mandates also are responsible for the tasks assigned to it.

Table 16: Epic Create open issue

5.2 First Acceptance

Epic Mandate situation	
Number	EPIC-009
Group	First Acceptance
Theme	Mandate Situation
Parent epic	-
Description	As group compliance officer I want to create and edit a mandate situation record in order to state the mandates' situation to date.
Resources	Figure 33: Create mandate situation
Comments	

Table 17: Epic Mandate situation

Epic Client situation	
Number	EPIC-010
Group	First Acceptance
Theme	Client Situation
Parent epic	-
Description	As group compliance officer I want to create and edit a client situation record in order to state the clients' situation to date.
Resources	Figure 34: Create client situation
Comments	

Table 18: Epic Client situation

Epic Versioning / Archive	
Number	EPIC-011
Group	First Acceptance
Theme	Versioning

Parent epic	-
Description	As a group compliance officer I want to create new versions of basic doc records (client and mandate) and documents whenever an accepted version has to be amended.
Resources	Figure 35: New version dialog windows Figure 36: Mandate archive overview
Comments	Manual (by human) as well as background versioning on status change can take place. Old versions are marked as archived and cannot be changed by anyone.

Table 19: Epic Versioning / Archive

Epic Workflows	
Number	EPIC-012
Group	First Acceptance
Theme	Workflows
Parent epic	EPIC-005, EPIC-006, EPIC-00
Description	As a group compliance officer I want to review and approve basic doc records and open issues in order to meet the internal regulatory and double check the information.
Resources	Figure 37: Workflow fields in basic doc Figure 43: Client status flow Figure 44: Mandate Status flows Figure 45: Open Issues Status flows
Comments	

Table 20: Epic Workflows

Epic Edit Open Issues	
Number	EPIC-013
Group	Review
Theme	Open Issues
Parent epic	EPIC-00
Description	As group compliance officer I want to edit and complete open issues in order to track and document tasks related to mandates.
Resources	-
Comments	

Table 21: Epic Edit Open Issues

5.3 Review

Epic Change of Account Managers	
Number	EPIC-044
Group	Review
Theme	Mandates
Parent epic	
Description	As a group compliance officer I want to change account managers on one or more mandates with a single action.
Resources	-
Comments	From A -> B (overall, selected mandates)

Table 22: Epic Change of Account Managers

Epic Transaction Management	
Number	EPIC-014
Group	Review
Theme	Transactions
Parent epic	-
Description	As a local or group compliance officer I want to document important transactions of a mandate by manually adding records to the database, based on bank statements.
Resources	Figure 46: Transaction Status flows
Comments	

Table 23: Epic Transaction Management

Epic Transaction Documents	
Number	EPIC-015
Group	Review
Theme	Documents
Parent epic	EPIC-007
Description	As a local or group compliance officer I want to add electronic documents like bank statements to transaction records of a mandate in order to have a proof of the transaction.
Resources	-
Comments	Document Management features as with client and mandates.

Table 24: Epic Transaction Documents

5.4 Name-Check

Epic Weekly Name-Check	
Number	EPIC-016
Group	Name Matching
Theme	Automated Name Check
Parent epic	-
Description	As a group compliance officer I want to the system to check all relevant names from clients individual & legal, mandates and transactions on a regular (currently weekly) basis.
Resources	-
Comments	*Relevant* in this case means all new, changed and unprocessed data in terms of the rating procedure.

Table 25: Epic Weekly Name-Check

Epic Full Name-Check	
Number	EPIC-017
Group	Name Matching
Theme	Automated Name Check
Parent epic	-
Description	As a privileged group compliance officer I want to the system to check all available names from clients individual & legal, mandates and transactions upon request.
Resources	
Comments	Basically identical with EPIC-016 but checks all available data regardless of the status in the rating procedure.

Table 26: Epic Full Name-Check

Epic Name-Check Result Management	
Number	EPIC-018
Group	Name Matching
Theme	Result management
Parent epic	-
Description	As a group compliance officer I want to rate the results from the name-checks in order to identify matches from the TMF database with World-Check or Blacklist data. Furthermore the rated results should be excluded from periodic checks unless changes occur.
Resources	Figure 39: Name Matching Rating
Comments	For privileged group compliance a persistent rating feature ensures that false-positive hits never pop up again regardless of changes.

Table 27: Epic Name-Check Result Management

Epic Name-Check Protocols	
Number	EPIC-019
Group	Name Matching
Theme	Name Matching Protocols
Parent epic	-
Description	As a group compliance officer I want to view search protocol of all name searches done by either users or the system itself.
Resources	Figure 40: Name Matching Check Protocol Figure 41: World-Check Protocol
Comments	The application always creates name-check protocols automatically in the background once a check has been executed. Exceptions are simple name searches out of any context like client or mandate. Two kind of protocols exist: The Name Matching Check Protocol states all information on the check itself: who check what when and what were the results. The World-Check protocol states a single entry with all details from World-Check database as of date of the search. Important: In order to create a World-Check protocol there always must be a corresponding Name-Check protocol documenting the check itself!

Table 28: Epic Name-Check Protocols

Epic World-Check Data	
Number	EPIC-020
Group	Name Matching
Theme	Name-Check Data source
Parent epic	-
Description	As an application administrator I want to import, update and delete data records from the provided World-Check XML data files.
Resources	Sample XML files for new/updated records (world-check.xml) and deletions (world-check-deleted.xml). XSD files Descriptions of World-Check
Comments	(0) Data structure (1) Import

	(2) Deletions

Table 29: Epic World-Check Data

Epic Blacklists	
Number	EPIC-021
Group	Name Matching
Theme	Name-Check Data source
Parent epic	-
Description	As group compliance officer I want to add names to a TMF-Group own blacklist of persona-non-grata in order to get all of those hits in all name-checks like they would be in World-Check database.
Resources	Figure 42: Blacklist Entry
Comments	The data structure should be the same as with World-Check data sets (XML), but with CRUD actions the entitled users.

Table 30: Epic Blacklists

5.5 Exit

Epic Mandate inactivation	
Number	EPIC-022
Group	Exit
Theme	Mandate
Parent epic	EPIC-006
Description	As a group compliance officer I want to inactivate a mandate in order to reflect the closed business relation according to the exit sheet.
Resources	-
Comments	Includes link inactivation to clients and mandates, consistency checks needed.

Table 31: Epic Mandate inactivation

Epic Client inactivation	
Number	EPIC-023
Group	Exit
Theme	Client
Parent epic	EPIC-005
Description	As a group compliance officer I want to inactivate a client in order to reflect the closed business relation according to the exit sheet.
Resources	-
Comments	Includes link inactivation to clients and mandates, consistency checks needed.

Table 32: Epic Client inactivation

5.6 Basic Applications

Epic Country Management	
Number	EPIC-024
Group	Basic Applications
Theme	Countries
Parent epic	-

Description	As an application user I want to have an up-to-date list of all countries worldwide so that it matches the ISO definition ISO 3166-1-alpha-2 code
Resources	List of countries “TMF-SEO.NEXT-CountriesCodes-ISO 3166-1-alpha-2_final.xlsx”
Comments	http://www.iso.org/iso/country_names_and_code_elements

Table 33: Epic Country Management

Epic Business Code Management	
Number	EPIC-025
Group	Basic Applications
Theme	Business codes
Parent epic	-
Description	As an application owner I want to be able to maintain a list of business codes on my own.
Resources	List of current business codes “TMF-SEO.NEXT-BusinessCodes_final.xlsx”
Comments	Source / List of this codes has to be defined by TMF-Group. For migration issues a matching table old-new values has to be provided.

Table 34: Epic Business Code Management

Epic Currency Management	
Number	EPIC-026
Group	Basic Applications
Theme	Currencies
Parent epic	-
Description	As an application user I want to have an up-to-date list of all currencies worldwide so that it matches the ISO definition ISO 4217:2008 Alphabetic Code
Resources	-
Comments	http://www.currency-iso.org/en/home/tables/table-a1.html

Table 35: Epic Currency Management

Epic Exchange Rates Management	
Number	EPIC-027
Group	Basic Applications
Theme	Exchange Rates
Parent epic	-
Description	As an application user I want to use up-to-date exchange rates so that the system automatically calculates accurate amounts of foreign currencies
Resources	-
Comments	http://www.oanda.com/currency/

Table 36: Epic Exchange Rates Management

5.7 Export/Report

Epic Data export	
Number	EPIC-029
Group	Export/Report
Theme	Data export
Process	-

Parent epic	-
Description	As a user I want to be able to export data from the system to be used in other systems.
Resources	-
Comments	New functionality as replacement of several Crystal Reports in SEO

Table 37: Epic Data export

Epic Data report / list views	
Number	EPIC-030
Group	Export/Report
Theme	Data report
Process	-
Parent epic	-
Description	As a user I want to be able to view data from the system in a predefined manner.
Resources	-
Comments	Simple list views like mandates per office or tasks, manageable by the application administrator. This epic needs further investigation how to cover this exactly.

Table 38: Epic Data report / list views

5.8 Application Search

Epic Basic search	
Number	EPIC-031
Group	Application search
Theme	Search
Process	-
Parent epic	-
Description	As a user I want to be able to search for any text all over the application.
Resources	-
Comments	Includes indexing of content (mainly list and form data). Optionally document attachment data if available (indexable content).

Table 39: Epic Basic search

Epic Advanced search	
Number	EPIC-032
Group	Application search
Theme	Search
Process	-
Parent epic	EPIC-031
Description	As a user I want to be able to search for specific elements in a defined context and filter my results.
Resources	-
Comments	Search parameters and filters may narrow the result set.

Table 40: Epic Advanced search

5.9 Security

Epic Authentication	
Number	EPIC-033
Group	Security
Theme	Authentication
Process	-
Parent epic	-
Description	As a user I want to be able to login with my windows account information
Resources	
Comments	The authentication of user must be done by using the TMF Domain Active Directory. No other directory must be used. If generally provided by SharePoint infrastructure, Single-Sign-On would be a nice to have benefit.

Table 41: Epic Security

Epic Authorization	
Number	EPIC-034
Group	Security
Theme	Authorization
Process	-
Parent epic	-
Description	As an application administrator I want to be able to assign access rights to users of the application.
Resources	
Comments	Roles can be assigned to user groups or users from the AD. Access rights in the application are assigned based on these roles. The following roles are predefined by the application: see 3.5. Specific rights for these roles should be predefined in the application, no configuration interface for the application administrator is needed.

Table 42: Epic Authorization

Epic Encryption	
Number	EPIC-035
Group	Security
Theme	Encryption
Parent epic	-
Description	As an application owner and responsible for compliance I want to be sure that all confidential information is encrypted and non-readable to unauthorized people.
Resources	Architecture and Design
Comments	See list of fields for the definition of encrypted fields “TMF-SEO.NEXT-FieldList_final.xlsx”

Table 43: Epic Encryption

Epic Record/Document Access	
Number	EPIC-036
Group	Security
Theme	Encryption
Parent epic	EPIC-034

Description	As an application owner and responsible for compliance I want to be sure that every user of the system has appropriate access to all information in the system.
Resources	-
Comments	CRUD is not sufficient! Especially “Read” has to be differentiated into sections of a record like “view only first section or view only field XYZ”.

Table 44: Epic Record/Document Access

Epic User Access Logging	
Number	EPIC-037
Group	Security
Theme	Logging
Parent epic	-
Description	As a privileged GCO I want to be able to see who accessed what information on which time and date.
Resources	-
Comments	In legacy SEO this feature is called “Hit log”.

Table 45: Epic User Access Logging

Epic User Activity Logging	
Number	EPIC-038
Group	Security
Theme	Logging
Parent epic	-
Description	As a priviledged GCO I want to be able to see who amended which information on which time and date.
Resources	-
Comments	This refers to the so calls mutation log of SEO. In the context of a record, the application logs the modifications on the record. The values for “date/time”, “username”, “fieldname”, “oldvalue” and “newvalue” must be present, no exceptions are allowed. 20131130 – John Doe – Lastname – Old value: Miller New value: Mueller

Table 46: Epic User Activity Logging

5.10 Administration

Epic User Management	
Number	EPIC-039
Group	Administration
Theme	Users
Parent epic	EPIC-033
Description	As an application administrator I want to be able to manage SEO.NEXT users and groups.
Resources	-
Comments	Only application administrators should be allowed to add, edit and delete users from groups or role assignments. As this is a security concern, system administrators must be excluded (no access) from assigning users to groups.

	If not possible due to ADS administration policy, a workflow for access rights approval by application admins might be implemented.

Table 47: Epic User Management

Epic Objects and Links Management	
Number	EPIC-040
Group	Administration
Theme	Links
Parent epic	-
Description	As an application administrator I want to create, manage and inactivate links of different types to different objects (like clients, mandates…)
Resources	-
Comments	See 3.6

Table 48: Epic Objects and Links Management

Epic Term Management	
Number	EPIC-041
Group	Administration
Theme	Labels and terms
Parent epic	-
Description	As an application administrator I want to manage all field labels, terms or text modules used in the application by using a graphical user interface.
Resources	-
Comments	No similar functionality in SEO is existing now. Field description, general terms and other text components, which are used in the application, should be manageable by the application administrator so that he can centrally change common terms like “account manager” to “client entity manager” for example. All fields and labels then should take use the new term.

Table 49: Epic Term Management

Epic Risk settings	
Number	EPIC-047
Group	Administration
Theme	Risk management
Parent epic	-
Description	As an application administrator I want to manage risk criteria and categories in order to have up-to-date lists for proper risk management.
Resources	-
Comments	-

Table 50: Epic Risk settings

Epic Application Monitoring	
Number	EPIC-042
Group	Administration
Theme	Monitoring
Parent epic	-
Description	As a system administrator I want to be able to monitor the system and the application

	without access to confidential information.
Resources	-
Comments	Server and database monitoring

Table 51: Epic Application Monitoring

Epic System Logging	
Number	EPIC-043
Group	Administration
Theme	Logging
Parent epic	-
Description	As a system administrator I want to be able to check and read system and application logs without access to confidential information.
Resources	-
Comments	Server and database maintenance

Table 52: Epic System Logging

5.11 Other

Epic Print	
Number	EPIC-045
Group	Other
Theme	Printing
Parent epic	-
Description	As a compliance user I want to be able to print list views from the system in a useful way in order to create internal documents for paper based workflows.
Resources	-
Comments	Generally SharePoint Print capabilities have to be used. Printing of large lists in a “data export” likely manner has to be limited to privileged users similar to real data export features.

Table 53: Epic Print

Epic Layout and Style	
Number	EPIC-046
Group	Other
Theme	Layout
Parent epic	-
Description	As a user I want to have a SharePoint-like behavior in the color and styles according to TMF-Groups’ CICD.
Resources	Color codes (RGB): Grey: R 69|G 85|B 96 Red: R 238|G 53|B 36
Comments	No CICD definition available

Table 54: Epic Layout and Style

6 User stories

User stories are documented in the spreadsheet “**TMF-SEO.NEXT-UserStories_final.xlsx**”. Selected stories need more specification or visualization, these are covered within this chapter.

6.1 Risk management

Key	Risk category
-	
A	Category A (low)
B	Category B (mid)
C	Category C (high)
D	Category D (very high)

Table 55: Risk categories

Key	Risk assets
-	
1	<2 MIO €
2	2 - 10 MIO €
3	10 - 50 MIO €
4	>50 MIO €

Table 56: Risk assets

Key	Risk criteria	Assigned category
->	Export from production system needed	

Table 57: Risk criteria

6.1.1 Risk management process

1. System: Auto-create risk criteria based on client links (PEP)
2. System: Auto-create risk criteria based on mandate type (services)
3. System: Auto-assign risk category according to criteria assigned
4. Human: Review risk criteria, add all relevant
5. Human: Assign risk asset values and countries
6. Human: Defunct (inactivate) auto-assigned risk category (if necessary)
7. System: Propose new category according new set of risk criteria
8. Human: Accept or change new risk category

6.2 Name-Check

The following figure shall visualize the behavior of the periodic check (what to search).

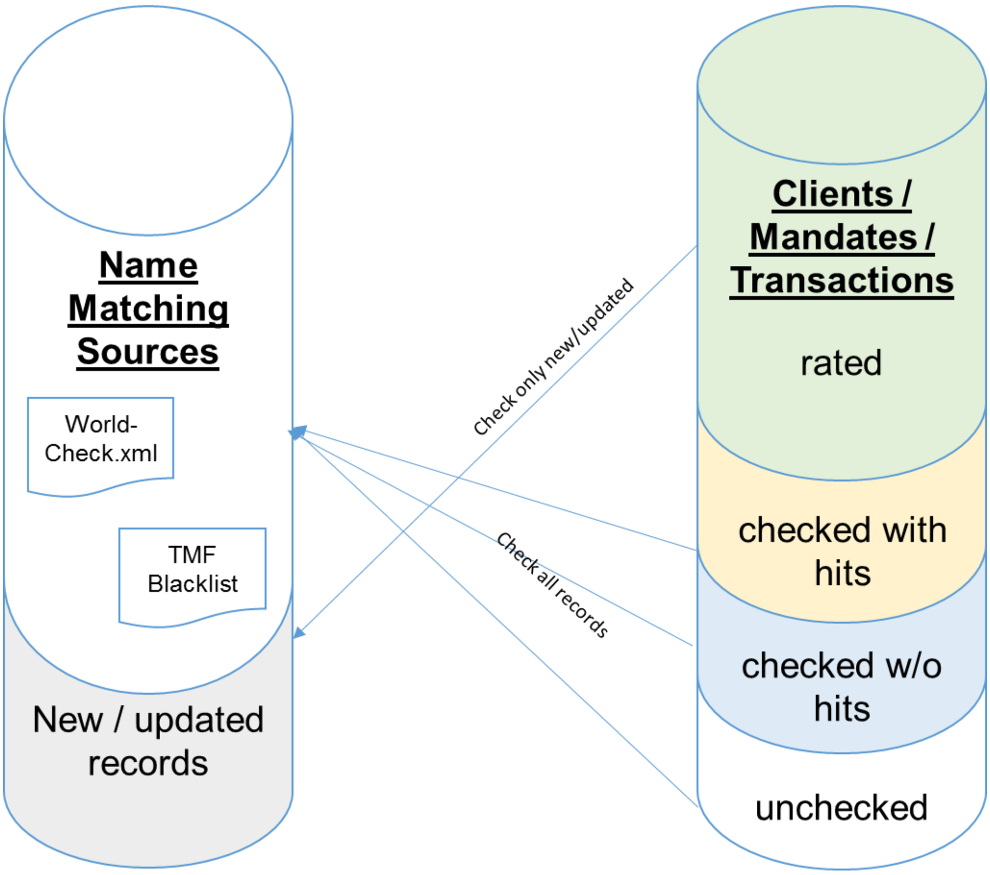


Figure 14: Name-Check

7 Non-functional (Quality) requirements

Nr	Category	Level	NFR
1	Availability	Org	Business days Mo-Fr (5*24) Mo-Fr 24*5 (CET) 0.50h = 99.5% uptime Weekends have generally the same availability but may be used for service maintenance windows for a maximum of 24h
2		Sys	System Availability (7*24) = 99.5% (unplanned interruptions)
3	Usability	Sys	The usability of the system has to fulfill the guidelines for SharePoint 2013 applications and match the current SEO experience as close as reasonable. If old behavior conflicts with SharePoint principles, SharePoint-like behavior is followed.
4	Security	Sys	As described in chapter 0 and 8.4
5	Performance	Sys	The following performance index must be fulfilled: • Max. response time for save of form data: 3s • Max. response time for load of form data: 2s • Weekly Word-Check on clients, mandates and transactions within 3 hours
6	Reusability	Sys	No specific requirement
7	Scalability	Sys	The system must be scalable to handle the following amount of data without impact on performance and stability: • 100’000 clients • 100’000 mandates • 750GB of document data • 200 concurrent active users
8	Platform independence	Sys	The system is bound to the Microsoft Windows server and SharePoint platform.
10	Serviceability	Sys	-
11	Stability	Sys	According to availability

Table 58: Non-functional requirements

7.1 Performance

in order to improve processing time following design decisions have been taken:

- Load balancer is used to distribute requests across the servers nodes (for the scalable deployment model).
- Use lazy loading fetch type for entity relationships.
- All views (overviews / lists) will display data per page - only required items to be displayed (10 items per page - configurable number) will be loaded from the business and persistence tiers components. Only required fields needed to be displayed to front end-users will be loaded from database.
- Reduce amount of data passed across tiers / components. Only mandatory data will be transferred.
- Connection pooling will be used for database access (optimal configuration for the pool).

- Use lazy loading data whenever a large amount of data is to be processed (download document). Only load binary and large data if explicitly required. Perform de-encryption on documents and business-data only if required.
- Use caching resources.
- Use the most appropriate isolation level for individual use cases : pessimistic vs. optimistic locking.
- Create indexed for SuD database tables (business data) considering the required ordering/searching.
- If necessary, system capacity could be increased by adding more raw processing power.
- Save of client basic doc - 2-3s
- Load of a mandate basic doc - 2s
- Weekly World-Check - less than 3h (cron job)

7.2 Scalability

in case of many new users join the SuD system - the system load will increase. With current design, SuD is prepared to increase scalability in both ways:

- Vertical scalability - adding more processing power in any of the servers outlined in the deployment diagram (affected resources: memory and processors; storage disks).
- Horizontal scalability - configuring and installing new nodes in the SuD environment which host the SuD software system (web & application servers / database servers).
- Database connectivity configured with connection pooling.

7.3 Reliability

(for scalable deployment model)

- SuD is designed with two load balancers servers: an active server and a stand-by server. If the active load balancer goes down the failover replaces it.
- SuD has WFE clustering with 2 server nodes and one hot-standby WFE server (active replication); SuD has Application Server clustering with 2 server nodes.
- SuD has database clustering with 2 server nodes (database servers) and one hot-standby database server.

7.4 Availability

SuD is 99.999% available by setting up redundant components and failover.

- SuD shall be 99.5% available from Monday to Friday (CET)
- Weekends are non-critical and may be used for service maintenance windows.
- For scalable deployment model, in order to avoid the system down time and long response time, SuD is designed with active replication (hot standby) for the WFE, Application Server and Database servers. This way the system availability is improved.
- The firewall and load-balancer are configured for failover, for scalable deployment model. The available capacity is handled by maintaining a stand-by server for firewall and load-balancer. Only one server is active at any given time. If the running server (firewall / load-balancer) goes down at any moment, the processes and state of that server are transferred to the failover server.

7.5 Extensibility

- SuD is designed with separation of concerns: Presentation Tier, Business Tier, Integration Tier.
- Each tier is loosely coupled with to the caller and called tier (interfaces and encapsulation).
- Adding additional functionality into a SuD's will have minimal impact (on existing components) based on the existing tiers. Additional functionality could be integrated in a specific tier (horizontal approach) or through all tiers (vertical approach).
- Integration of new languages will be rapidly supported by providing the appropriate resource file `.resx` (Share Point).

7.6 Maintainability

- Maintainability is supported with SuD good documentation (UML diagrams; technical notes).
- Code factoring - separation of responsibilities in the code: looser coupling, minimal dependencies and modularity - making the components and code more reusable.
- If there will be changes requests, they will only affect the specific components.

7.7 Manageability

- SuD is implemented with Share Point logging mechanism.
- In runtime, additional tool could be configure to watch the SuD log files and alert/notify an administrator when log-messages with FATAL or ERROR level occur.
- Share Point Services Management & Control.

7.8 Security

SuD's security is designed to maintain the security contexts in all tiers.

- Share Point security authentication & permissions/authorization at any level.
- Parameters tampering & defensive programming : web (encrypted parameters) and business component (check values).
- Share Point prevents all known XSS attacks.
- Flows injections (SQL) - no SQL gets executed by simply concatenating directly the values typed by the user.
- All uploaded files stored in the SuD database will be encrypted before saving. No uploaded & un-encrypted document will be temporarily stored. Uploading and encryption is done in memory be fore persisting documents in database (Share point Document Management System - repository

Architecture and Design

8 UML diagrams

Current documentation contains the architecture and design for the SEO.NEXT, system under development (further referenced within this documentation as SuD).

8.1 Class diagram

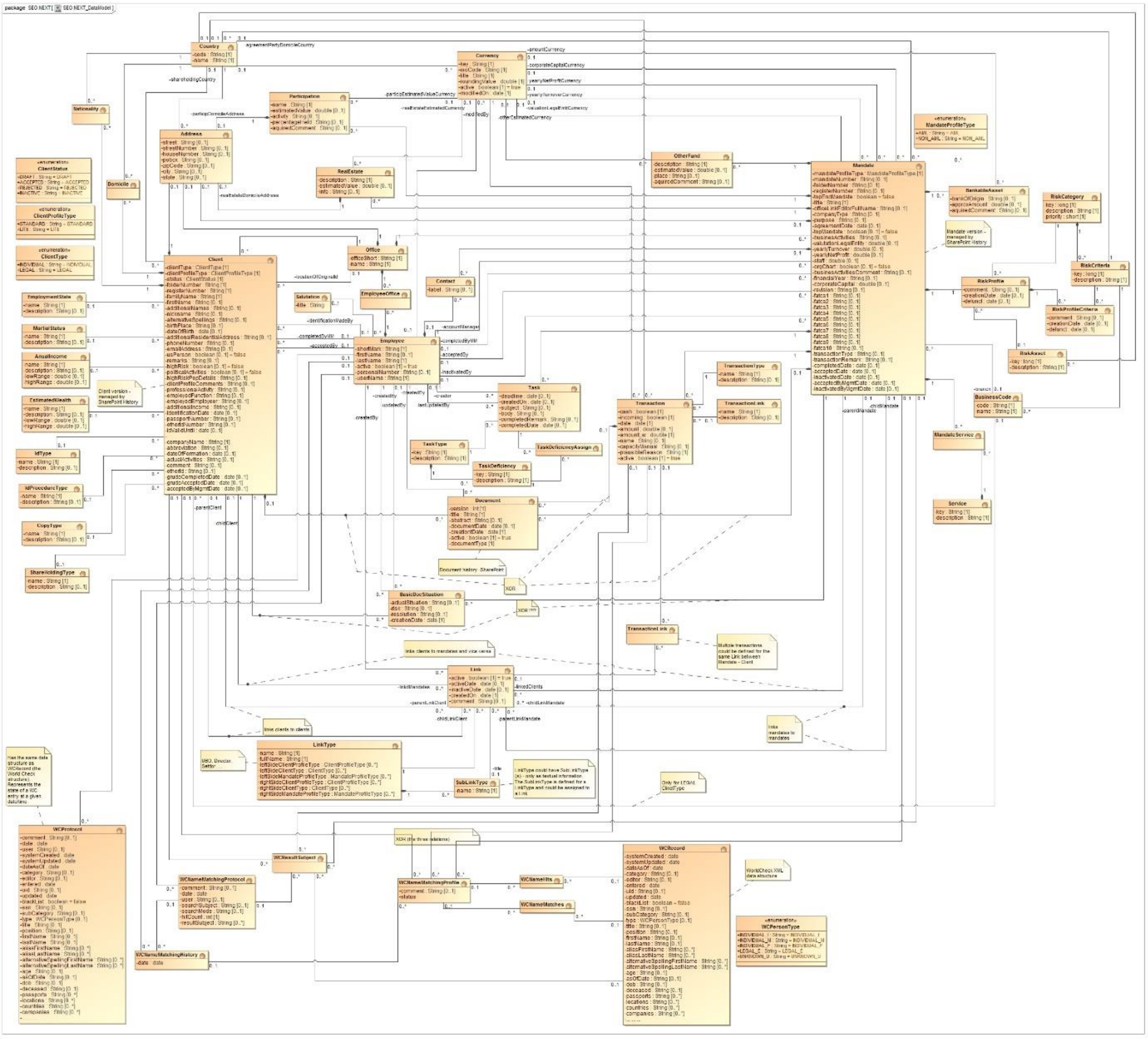


Figure 15: UML Class diagram

8.1.1 Entity classes specifications

- Employee entity does not store the system's users and does not hold the authentication and authorization properties. Each employee which is also a user must have a unique login (the userName property must match with the corresponding Active Directory user's identification). The 'employees' are specific users (from Active Directory system) assigned to a specific AD group - which grants access to the SEO.NEXT system. Employees belong to an Office or more. An office could have one or more local compliance (employee - user). There are situations where the same user (employee) is local compliance for more offices. Following roles are available for users: group compliance, local compliance by country, local management, group management, DCS. Each user has assigned one role which is loaded on the context after successful authentication. Based on the assigned role, the allowed/defined permissions are assigned to the logged-in user (SharePoint). User creation through SuD is not allowed. Users who should be able to access SuD shall be defined through the Active Directory external system.

- Office entity contains the basic properties of offices. Each offices belongs to a country. A mandate has single office; an office can have multiple mandates. Client can have multiple offices; office can have multiple clients.
- Client entity stores the properties for Individual clients (persons) and Legal clients (companies); From the technical perspective, Individual clients and Legal clients will be stored in the same table (multiple common properties), but flagged accordingly by the ClientType property. ClientProfileType defines the current client's profile. ClientStatus defines the current status of clients.
- Country, Currency, BusinessCode, LinkType, LinkCategory, Service, RiskCategory, RiskCriteria, RiskAsset, TaskType, TaskDeficiency, ... represent SuD administrative tables..
- EmploymentState, MartialStatus, IdType, IdProcedureType, CopyType, ShareHoldingType client specific administrative data lists (are handled in the SuD as SharePoint lists).
- AnualIncome, EstimatedWealth administrative encrypted data tables.
- Mandate table holds the customers' data for which TMF offers services. Each mandate has a MandateProfileType which defines the current profile type (see the ClientProfileType for clients).
- Link defines the links between Clients - Mandates; Clients - Clients; Mandates - Mandates by using the appropriate relations.
- LinkType defines the type of the links between Clients and Mandates by using the ClientProfileType and MandateProfileType definitions. For each LinkType there should be defined the left and the right side - which defines the relation/link between Client-Mandate; or Client-Client; or Mandate-Mandate.

For example:
1. The following LinkType could be defined (Application Administrator) in order to allow mapping of Clients (standard OR lite) OR Mandate (AML) with Clients (standard) OR Mandate (NON-AML):

Left side	Right side
ClientProfileType: `STANDARD` OR `LITE`	ClientProfileType: `STANDARD`
MandateProfileType: `AML`	MandateProfileType: `NON-AML`

2. The following LinkType could be defined to define UBOs (doesn't allow Mandate to Mandate; doesn't allow Client to Client):

Left side	Right side
ClientProfileType: `STANDARD`	ClientProfileType:
MandateProfileType:	MandateProfileType: `AML`

3. The following LinkType could be defined to define UBLs :

Left side	Right side
ClientProfileType: `LITE`	ClientProfileType:
MandateProfileType:	MandateProfileType: `NON-AML`

- For a LinkType there could exist none/one/more SubLinkType entities - which only provide textual information. SubLinkType belongs (is defined for a LinkType) and it could be assigned to a Link. For example, SuD could have defined the Link 'OTHER RELATION' and the SubLinkType : 'FRIEND' 'KID'.

- Nationality & Domicile tables define the country related nationality and domicile for Clients.
- MandateService allows configuration of the Services for Mandates.
- BankableAsset, Participation, RealEstate, OtherFund represent the Mandate related funds.
- Address entity holds the address data for Clients, Offices, Mandates, RealEstate (domicile), Participation (domicile). In some of the cases, the addresses data is encrypted (Clients, Mandates, ...).
- Document entities are managed by the Document Management System - Share Point service. The uploaded documents are encrypted before being stored into the database. SuD should always know about the original size in bytes of the uploaded document. A document could exist in the SuD because of being assigned to a Client, Mandate or Transaction. The DocumentType defines the the type of document based on the relation between Document and Client-Mandate-Transaction.
- ClientHistory, MandateHistory, DocumentHistory are handeled in the SuD by SharePoint history service (manage different versions).
- HitLog (not represented in the UML diagram) - shall keep tracking of all the actions (read/write mode) to all the entities (SharePoint).
- MutationLog (not represented in the UML diagram) - shall keep tracking of all the changes - 'who did change?' & 'what changed? from what to what?'. Keeps tracking of changing the status for Clients, Mandates and Documents when status changed from ACCEPTED to DRAFT; OR CREATE_NEW_VERSION For example, if there is a Client in status ACCEPTED, then this client is in ReadOnly mode for any user (no user can do changes to this client). If a user wants to change such a client (ACCEPTED), the user must first create a new version and the changes could only be applied on the new version.
- Transaction could be defined between Mandate and Client (existing in SuD); or between Mandate and a different company which does not exist in SuD.
- Task defines the Mandate's tasks. TaskDeficiencyAssign defines which of the selected TaskDeficiency (-ies) through the TaskType should be available for the Task.
- RiskCriteria defines the Mandate's risks. A user could assign N (5) RiskCriteria from 3 different RiskCategory to the Mandate's RiskProfile ==> in this case SuD automatically detects the RiskCategory based on the highest priority. Still the SuD shall allow user to change the predefined/suggested RiskCategory to a different one.
- WCRecord represents the the WorldCheck data structure based on the periodically recieved XML files (see world-check-day.xml file). This table will be periodically updated by the cron-job (which runs periodically) which reflects the changes occured into the latest version of the XML file.
- WCNameMatchingProtocol reflects all the checks (searches) which are done against the WorldCheck existing data. If user checks for 'John' on 08.01.2014, then the SuD will protocol (store) this check (who did the check, when, number of hits, comment). The same protocol is done when SuD automatically runs the cron job and detects changes. SuD takes data from the database (mandates, clients, transactions) and searches through latest XML version data. The search is also done against the 'Black List' - which represents entries into the WCRecord flagged as being black-listed.(Head Group Complience only can manually decide weather a Client should be in the black list or not (this is an individual decision). WorldCheck does not specify if a person is in the Black List; WorldCheck just specifies the category: category="TERRORISM". Even if a WorldCheck record has assigned a good category, it could be marked as BlackList in SuD.
- WCProtocol represents an WorldCheck entry (WCRecord) protocolled at a given date/time (it is a snapshot of the data at the current time when the searching has been done). Next day the

search results could be different. By having the protocol, user can find the difference between the different dates the search has been done.

- WCNameMatchingProfile allows users to define/rate matching between existing data (Clients, Mandates and Transactions - through WCResultSubject) and latest WorldCheck set of data (periodically). Once a client is rated - it will be excluded from matching until related WorldCheck data/record will change or user changes the related entry into SuD, or new hits show up at search. This way, SuD reduces work which for users who have to do the matching periodically (any time a new set of data is available from World Check).

8.1.2 Encrypted fields

Follow fields must be encrypted before being persisted into the database:

Entity	Encrypted Fields
Client INDIVIDUAL	familyName, firstName, additionalNames, nickname, alternativeSpellings, placeOfBirth, additionalResidentialAddress, phoneNumber, emailAddress, remarks, highRisksPepDetails, clientProfileComments, professionalActivity, employedFunction, employedEmployeer, additionalIncome, passportNumber, otherIdNumber, idValidUntil Address:street, streetnumber, zipCode, city
Client LEGAL	companyName, abbreviation, remarks, highRisksPepDetails, clientProfileComments, actualActivities, comment Address:street, streetnumber, pobox, zipCode, city
AnualIncome	name, description, lowRange, highRange
EstimatedWealth	name, description, lowRange, highRange
Mandate	title, officeLinkEditorFullName, companyType, purpose, topEndMandate, businesActivities, businesActivitiesComment, financialYear, corporateCapital, revision, transactionType, transactionRemark Address:street, streetnumber, zipCode, city
BankableAsset	bankOfOrigin, approxAmount, aquiredComment
Participation	name, estimatedValue, activity, percentageHeld, aquiredComment Address:street, streetnumber, zipCode, city
RealEstate	description, estimatedValue, info Address:street, streetnumber, zipCode, city
OtherFund	description, estimatedValue, place, aquiredComment
Link	comment
Document	title, abstract
Transaction	amount, amountLW, name, capacityManual, plausibleReason
Task	subject, body, completedRemark
BasicDocSituation	actualSituation, risk, resolution
RiskCategory	description
RiskAsset	description
RiskCriteria	description
RiskProfileCriteria	comment
RiskProfile	comment

- The ForeignKeys between tables with encrypted values are not to be encrypted.

- All encrypted and searchable fields must support search functionalities.
- All Documents must be encrypted before being stored into the SharePoint - Document Management System - Repository.

8.2 Component diagram

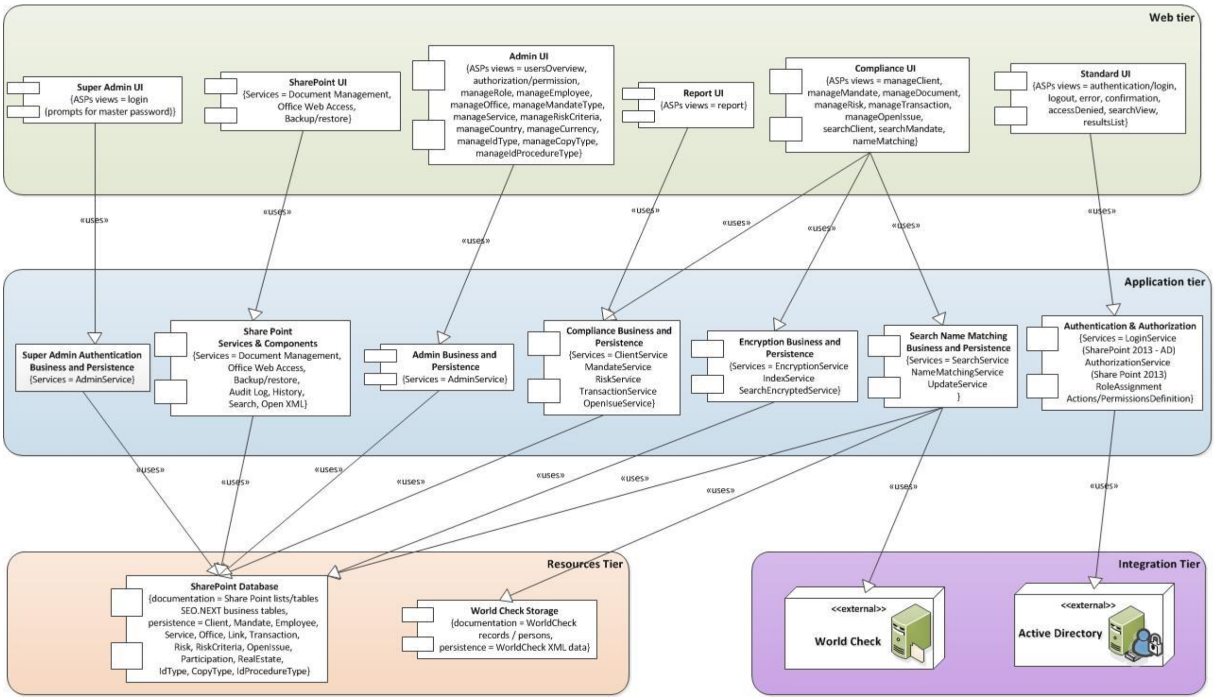

Web tier
Super Admin UI
{ASPs views = login
(prompts for master password)}
SharePoint UI
{Services = Document Management,
Office Web Access,
Backup/restore}
Admin UI
{ASPs views = usersOverview,
authorization/permission,
manageRole, manageEmployee,
manageOffice, manageMandateType,
manageService, manageRiskCriteria,
manageCountry, manageCurrency,
manageIdType, manageCopyType,
manageIdProcedureType}
Report UI
{ASPs views = report}
Compliance UI
{ASPs views = manageClient,
manageMandate, manageDocument,
manageRisk, manageTransaction,
manageOpenIssue,
searchClient, searchMandate,
nameMatching}
Standard UI
{ASPs views = authentication/login,
logout, error, confirmation,
accessDenied, searchView,
resultsList}
«uses»
Application tier
Super Admin Authentication
Business and Persistence
{Services = AdminService}
Share Point
Services & Components
{Services = Document Management,
Office Web Access,
Backup/restore,
Audit Log, History,
Search, Open XML}
Admin Business and
Persistence
{Services = AdminService}
Compliance Business and
Persistence
{Services = ClientService
MandateService
RiskService
TransactionService
OpenIsueService}
Encryption Business and
Persistence
{Services = EncryptionService
IndexService
SearchEncryptedService}
Search Name Matching
Business and Persistence
{Services = SearchService
NameMatchingService
UpdateService
}
Authentication & Authorization
{Services = LoginService
(SharePoint 2013 - AD)
AuthorizationService
(Share Point 2013)
RoleAssignment
Actions/PermissionsDefinition}
Resources Tier
SharePoint Database
{documentation = Share Point lists/tables
SEO.NEXT business tables,
persistence = Client, Mandate, Employee,
Service, Office, Link, Transaction,
Risk, RiskCriteria, OpenIssue,
Participation, RealEstate,
IdType, CopyType, IdProcedureType}
World Check Storage
{documentation = WorldCheck
records / persons,
persistence = WorldCheck XML data}
Integration Tier
<<external>>
World Check
<<external>>
Active Directory

Figure 16: UML Component diagram

8.2.1 Considerations

- The `Super Admin UI & Business and Persistence` component prompts for the master password any time the SuD reboots and enables SuD for end-users. The authentication is not done against the Active Directory external server. See the Encryption Component for details.
- `SharePoint native functionalities` : Document management, Workflows (without Nintex), Office Web Access - provide preview of encrypted-decrypted documents and avoid traffic (read mode only - no additional license needed for read only mode; if editing will be required - additional license would be needed). Backup / restore (scheduler - if required), Audit Log (logs all actions into DB), History (for documents and DB records; track differences between different versions "what / who / when" - did the changes).
- The `Admin UI & Business and Persistence` components offers management functionalities (CRUD - create, read, update, delete) for the SEO.NEXT's lists/entities, persisted in the SharePoint - SEO.NEXT database (lists and business entities).
- The `Authentication and Authorization` component (Share Point) secures the access to system by using the external Active Directory system. Authentication (integration with Active Directory), Authorization (Share Point native functionality) - permissions at any level: documents and records (DB level).
- The `Encryption Business and Persistence` is the central component for all other components that have to deal (encrypt / decrypt) with sensitive data. Whenever a new client, mandate, open issue, transaction or other sensitive data is being created or edited; the data will be processed (encrypted) by this encryption component before being persisted into the

database. For displaying encrypted data to front end users, this component will access encrypted data, decrypt the data and make it available in the current session for the user. In order to search through encrypted data, this component will be used for creating the in-memory search index.

- The `Compliance UI & Business and Persistence` components manage (CRUD - create, read, update, delete) the related business entities (clients, mandates, transactions, open issues, ...).
- The `Report UI` component provides a very limited number of structured reports (Open issues). Each user profile will have dashboard / management views that will show what is most important to them, with some drilldown capability. Local compliance officers will be able to 'dump' all their visible mandate data into an unformatted excel output. This would contain all the business relevant information in the database. Equally Group Compliance will be able to do the same, inclusive of UBOs/Directors. Some basic filters will be provided to the feature to generate the dumps.
- The `World Check Storage` component refers the client data (currently does not refer to mandates) fetched from the World Check external system as XML format. All the information/data obtained from World Check is not encrypted.
- The `Search Name Matching` component must search through encrypted and unencrypted (in memory-index) data. The 'search' does not have to consider the encrypted documents.
- All uploaded documents are encrypted and stored into Share Point's Document Management System repository.

8.3 Deployment diagram

8.3.1 Standard Deployment Diagram

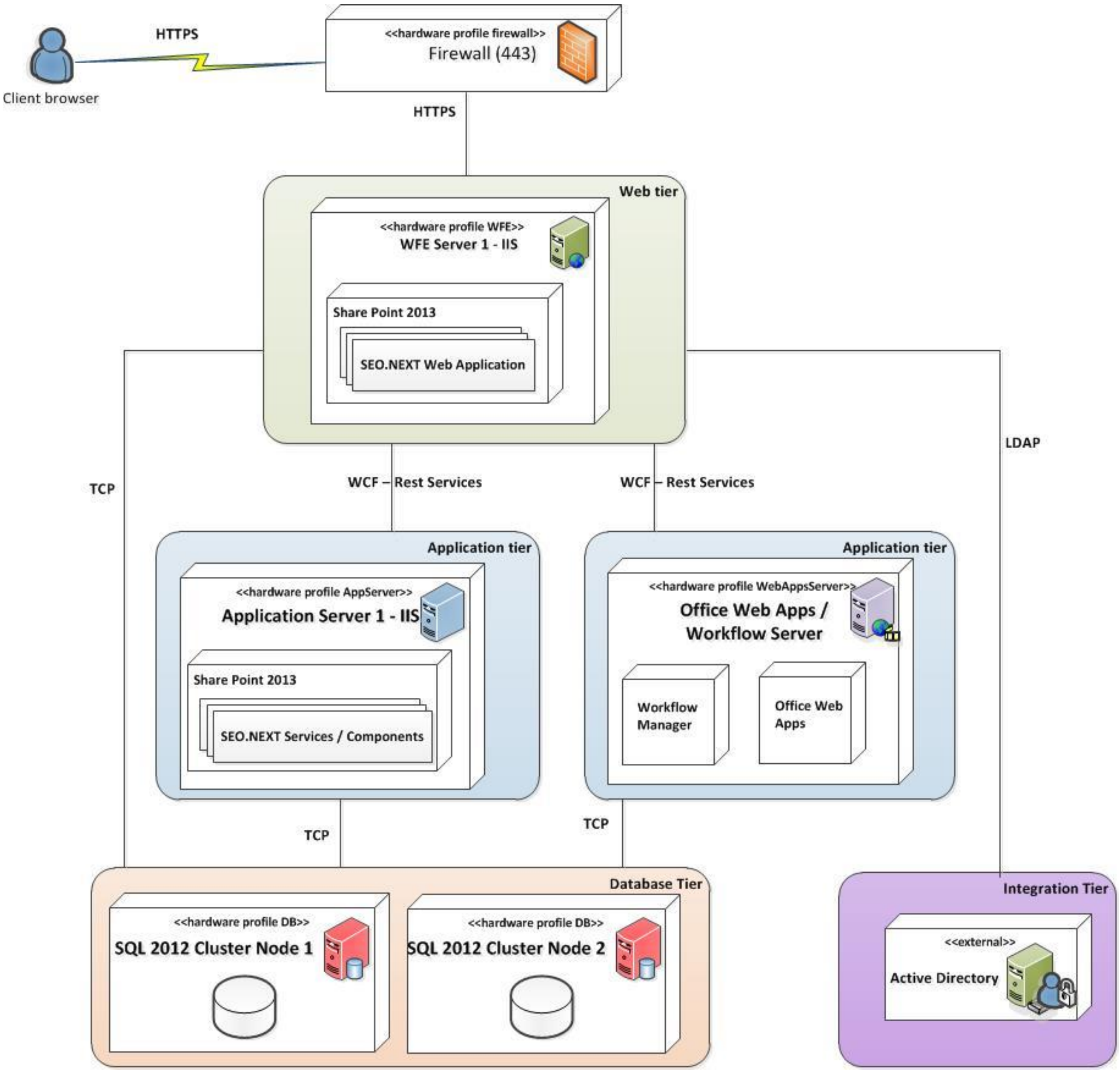


Figure 17: Standard deployment diagram

8.3.2 Considerations

- SuD will run in the private cloud (SuD network with all machines and services configured for SuD purpose) explicitly designed for its deployment.
- For testing and QA purpose, two different environments (development environment and test environment) could be setup.
- Round-Robin algorithm is configured to be used on the Load balancer component.
- hardware profile firewall `Juniper SSG-520`
  `SSG 520 System,`
  `1GB DRAM,`
  `AC Power - SSG-520-001`

- hardware profile WFE IIS +7 Server
  ```
  Share Point 2013 Standard Edition
  os: Windows Server 2008 R2 Enterprise Edition x64

  Application server
  - Dell PowerEdge R710 Servers
  - 4 core Intel® Xeon® X5570 Processors
  - 24 GB RAM, 3.2 GHz

  Storage is not a concern.
  ```

- hardware profile AppServer IIS +7 Server
  ```
  Share Point 2013 Standard Edition
  In-memory Index
  os: Windows Server 2008 R2 Enterprise Edition x64

  Application server
  - Dell PowerEdge R710 Servers
  - 4 core Intel® Xeon® X5570 Processors
  - 24 GB RAM, 3.2 GHz

  Storage is not a concern.
  ```

- hardware profile WebAppsServer os: Windows Server 2008 R2 Enterprise Edition x64
  ```
  Application server
  - Dell PowerEdge R710 Servers
  - 4 core Intel® Xeon® X5570 Processors
  - 16 GB RAM, 2.4 GHz
  ```

- hardware profile DB SQL Server 2012 Enterprise Edition
  ```
  os: Windows Server 2008 R2 + x64 (Windows 7 SP 1)

  Database server
  - Dell PowerEdge R710 Servers
  - six-core Intel® Xeon® Processor 5645
  - 64 GB RAM, 8M Cache, 3.20 GHz
  - 2 x Fusion-io®1000IDSS 1,000GB (1TB) ioDrive PCIe solid state
  storage car RAID 1
  - Broadcom 5709 1GbE quad-port NIC (LAN on motherboard)
  - 2 x Broadcom NetXtreme II 57711 10GbE NIC, Dual-Port

  Virtualization server (optional)
  - Dell PowerEdge R610 Servers:
  - System BIOS version 2.0.11
  - six-core Intel® Xeon® Processor 5645
  - 64 GB RAM, 8M Cache, 3.20 GHz
  - 2 x 149 SSD RAID1
  - Broadcom 5709 1GbE quad-port NIC (LAN on motherboard)

  Network
  - 2 x Dell PowerConnect 6248 1Gb Ethernet Switch
  - 2 x Dell PowerConnect 8024F 10Gb Ethernet Switch

  Storage (hardware profile FS specific):
  - Up to Twenty-four (24) 3.5" SAS, NL SAS and SSD
  - 2.5" Drive Performance and Capacities
  - 24 X Solid State Drive (SSD) available in 149GB (available in 3.5"
  ```

```
HDD carriers)
- Raid 10
```

- SEO.NEXT system study case:
  - considering number of users = 1,000
  - considering number of mandates = 100,000
  - considering number of clients = 100,000
  - considering the average size of uploaded documents into SuD is up to 0.25 MB --> encrypted documents will be up to 0.4 MB
  - considering the maximum size of document uploaded into SuD is up to 20 MB
  - considering SuD has an average number of 4 documents for one client
  - considering SuD has an average number of 15 documents for one mandate
  - SuD keeps all the uploaded documents for the lifetime of the client / mandate
  - considering most users are located in different time zones, the most pessimistic estimation number of concurrent users is 100

Based on the above considerations, the following storage and RAM configuration decisions have been taken, to outline that SuD will adequately scale and perform:

- Storage decision configuration : considering the above numbers, the size of the storage disk should be around 500 GB.

```
160,000 MB for clients documents  (100,000 x  4 x 0.4MB)
600,000 MB for mandates documents (100,000 x 15 x 0.4MB)
 10,000 MB for all business data

Total: 770,000 MB (770 GB)
```

- RAM (24 GB RAM in hardware profile WFE and AppServ): Most consumption memory will be in case of "download document" of a mandate/client (involves de-encryption). In most pessimistic case, each user needs around 25 MB (20 MB + encryption/decryption processing) at runtime (considering user selects to load/view biggest attachment). 200 concurrent users * 25MB = 5 GB. For worse scenarios (just in case), where number of concurrent users increases to 300 users and memory used for each user goes up to 50 MB, used RAM will be 15 GB. Considering that Share Point resources consumption is high enough; servers 100% overloading must be avoided, that is why a buffer is considered in here.

8.3.3 Scalable Improvement Model

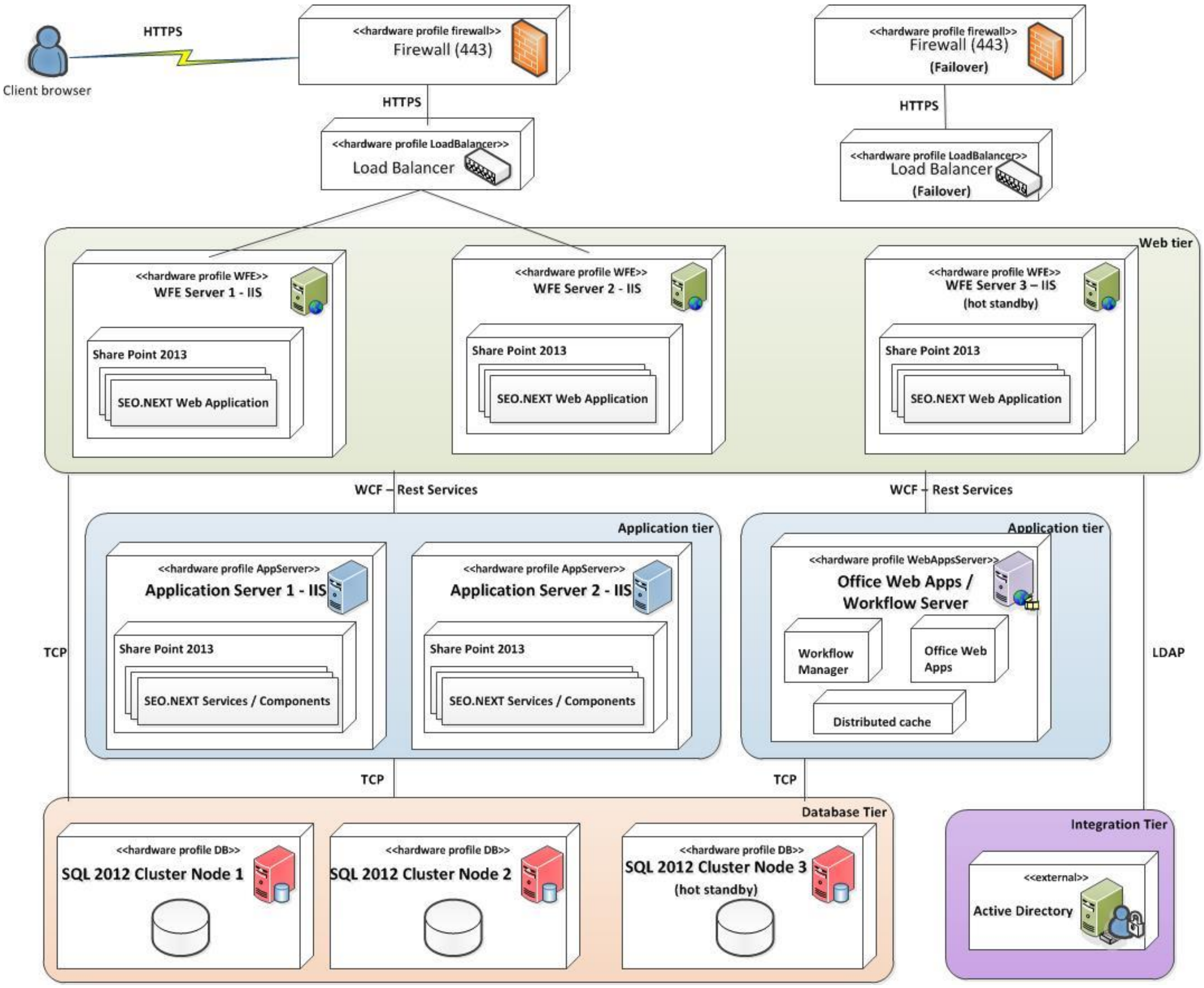


Figure 18: Scalable improvment model diagram

- hardware profile LoadBalancer Software (Apache, Nginx, HAproxy) or Hardware (F5, Barracuda, ...) Load Balancer solutions could be used (budget dependent).

  Software:
  ```
  Apache HTTP Server 2.4.x

  Application server
  - Dell PowerEdge R710 Servers
  - 2 x Quad Core Intel® Xeon® X5570 Processors
  - 8 GB RAM, 2.8 GHz

  Storage is not a concern.
  ```

  Hardware:
  ```
  Barracuda Load Balancer ADC 340
  Maximum Throughput 1 Gbps

  Technicla specs
  - Layer 4 & Layer 7 load balancing
  ```

- IPv6/IPv4 support
- Default load balancing: Round robin; Weighted round robin; Least connection
- Protection against common attacks: OWASP Top 10; SQL injections; Cross-site Scripting; Cookie or form tampering
- Supported Protocols: HTTP/S, SSH, SMTP, IMAP, POP3, NNTP, ASP, DNS, LDAP, RADIUS, TFTP, RDP, Windows Terminal Services, Any TCP/UDP application Storage is not a concern.

The Software LB solution is recommended (sticky session configuration). The DNS will be configurred on a virtual IP which will automatically switch to the other LB as soon as the first LB will become inactive (Corosync si Pacemaker).

8.3.4 Simplified Deployment Model

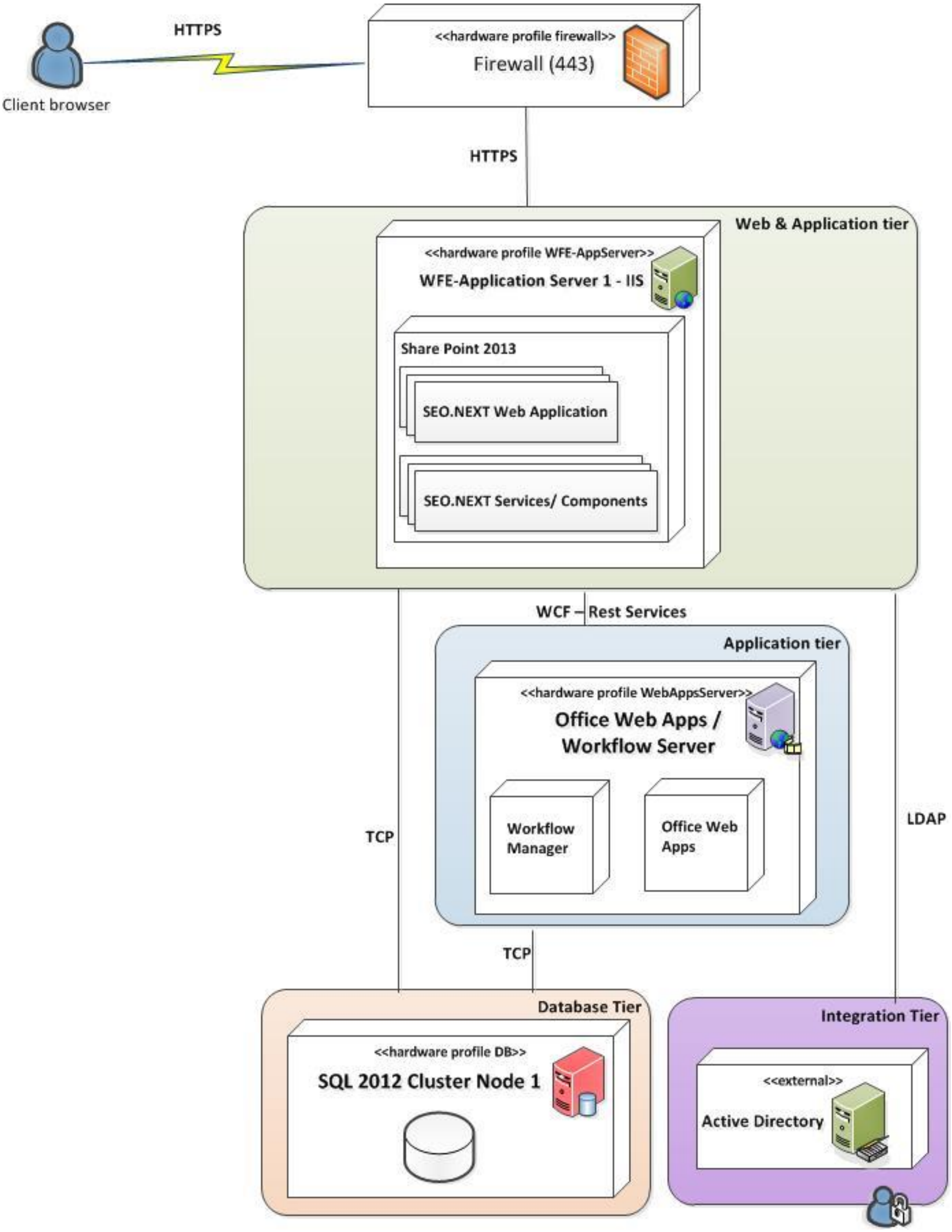


Figure 19: Simplified deployment model diagram

- hardware profile WFE-AppServer `IIS +7 Server`
  `Share Point 2013 Standard Edition`
  `In-memory Index`

```
os: Windows Server 2008 R2 Enterprise Edition x64

Application server
- Dell PowerEdge R710 Servers
- 4 core Intel® Xeon® X5570 Processors
- 24 GB RAM, 3.2 GHz

Storage is not a concern.
```

8.4 Encryption

8.4.1 Encryption component

Data encryption, for documents and business entities (clients, mandates, open issues and transactions), will be integrated by customized components (no third-parties tools/solutions will be used):

- `Encryption Component` is the central component used for data encryption and de-encryption.
- `Encryption Component Persistence` represents the storage component for persisting the Public and Private Keys.
- `Super-Admin Authentication Component` always runs when SuD starts/reboots.

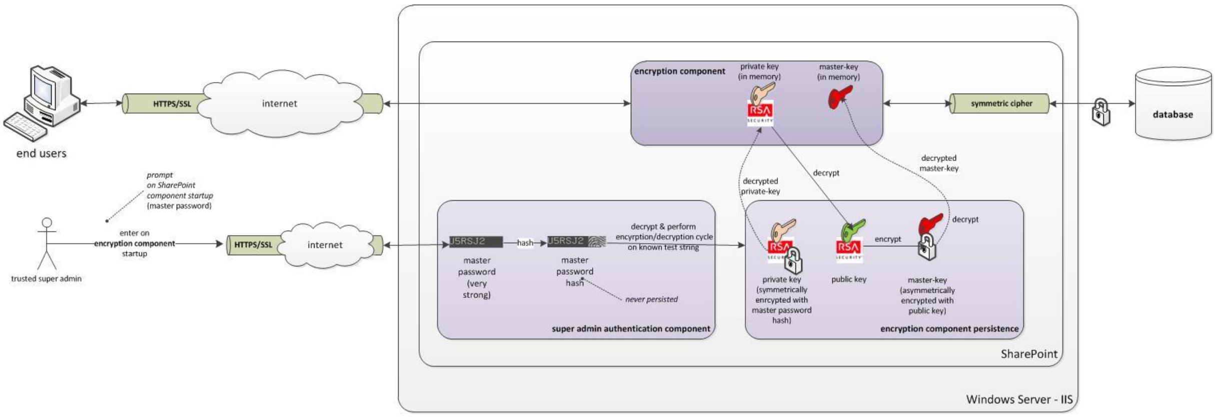

end users
HTTPS/SSL
internet
encryption component
private key (in memory)
master-key (in memory)
symmetric cipher
database
prompt on SharePoint component startup (master password)
trusted super admin
enter on encryption component startup
HTTPS/SSL
internet
J5RSJ2
hash
J5RSJ2
master password (very strong)
master password hash
decrypt & perform encyrption/decryption cycle on known test string
never persisted
super admin authentication component
decrypted private-key
decrypt
decrypted master-key
decrypt
encrypt
private key (symmetrically enrcypted with master password hash)
public key
master-key (asymmetrically encrypted with public key)
encryption component persistence
SharePoint
Windows Server - IIS

Figure 20: Encryption component diagram

- SuD will require the `master password` any time the system(s) reboots. The `master password` will be only known and provided by the `trusted super admin`. Until the `trusted super admin` doesn't enter the `master password` SuD is locked for all the end-users (independent of their roles) and no one can access the SuD. While SuD is disabled/locked, the only available/accessible page/functionality will be the page asking for the `master password`.
- The `master password` entered by the `trusted super admin` is processed by the `Super Admin Authentication Component` which validates the entered password (checks weather the `master password` is valid or not). If `master password` is incorrect SuD will ask again for the `master password`. SuD marks the super admin authentication state, in order to prevent password cracking attacks, where brute force is used to repeatedly attempt to login as a valid `trusted super admin` by guessing the `master password`. After a configurable number (5) of wrong login attempts, the SuD will be blocked for a configurable number of minutes (5). With the first successful login (after block period expired) the SuD is

unblocked.
After a successful authentication the `Encryption Component Persistence` and `Encryption Component` process the `master password` and get access to the Public and Private Keys; use the asymmetric keys and generate the Master Key . The Master Key is only kept in memory and it is used for encryption and de-encryption of documents/business-data. The process, of obtaining the Master Key is executed each time the system reboots. The asymmetric keys (Public and Private key) are PBE (password-based-encryption) - the `master password` will be converted to asymmetric keys (Public & private Keys).

- For the first time when SuD starts, there will be no asymmetric keys stored into the `Encryption Component Persistence` and therefore the validation for the `master password` could not be done. Because of this, for the first time only, SuD will automatically generate the Public and Private Keys based on the first entered `master password` (which should be considered as being correct/trusted).
- All the data (documents, clients, mandates, open issues, transactions) is encrypted with symmetric encryption algorithm (symmetric encryption is must faster than asymmetric encryption). Content (data) is encrypted with symmetric encryption and the keys for symmetric encryption are encrypted with asymmetric encryption algorithms.
  For encryption of documents/business-data based on `master password` SuD generates Public and Private Keys (asymmetric). The Public Key is used to generate the Key for symmetric encryption. With this Key (symmetric) `Encryption Component` encrypts the documents/business-data and saves them into database. The Public and Private Keys will be stored through the `Encryption Component Persistence`.
  For de-encryption of documents/business-data, SuD uses the Private Key to de-encrypt the Key for symmetric-encryption. With the Key (symmetric) SuD de-encrypts the documents/business-data.
- From the deployment perspective the three components are distributed as follows:
  `Super-Admin Authentication Component` lives in the `hardware profile AppServer` for Standard and Scalable diagrams; and lives in the `hardware profile WFE-AppServer` for the Simplified Deployment Model.
  `Encryption Component` lives in the `hardware profile AppServer` for Standard and Scalable diagrams; and lives in the `hardware profile WFE-AppServer` for the Simplified Deployment Model.
  `Encryption Component Persistence` lives in the `hardware profile AppServer` for Standard and Scalable diagrams; and lives in the `hardware profile WFE-AppServer` for the Simplified Deployment Model.

8.4.2 Master Password Validation

The Super Admin Authentication Component receives the master password in clear text and performs the validation:

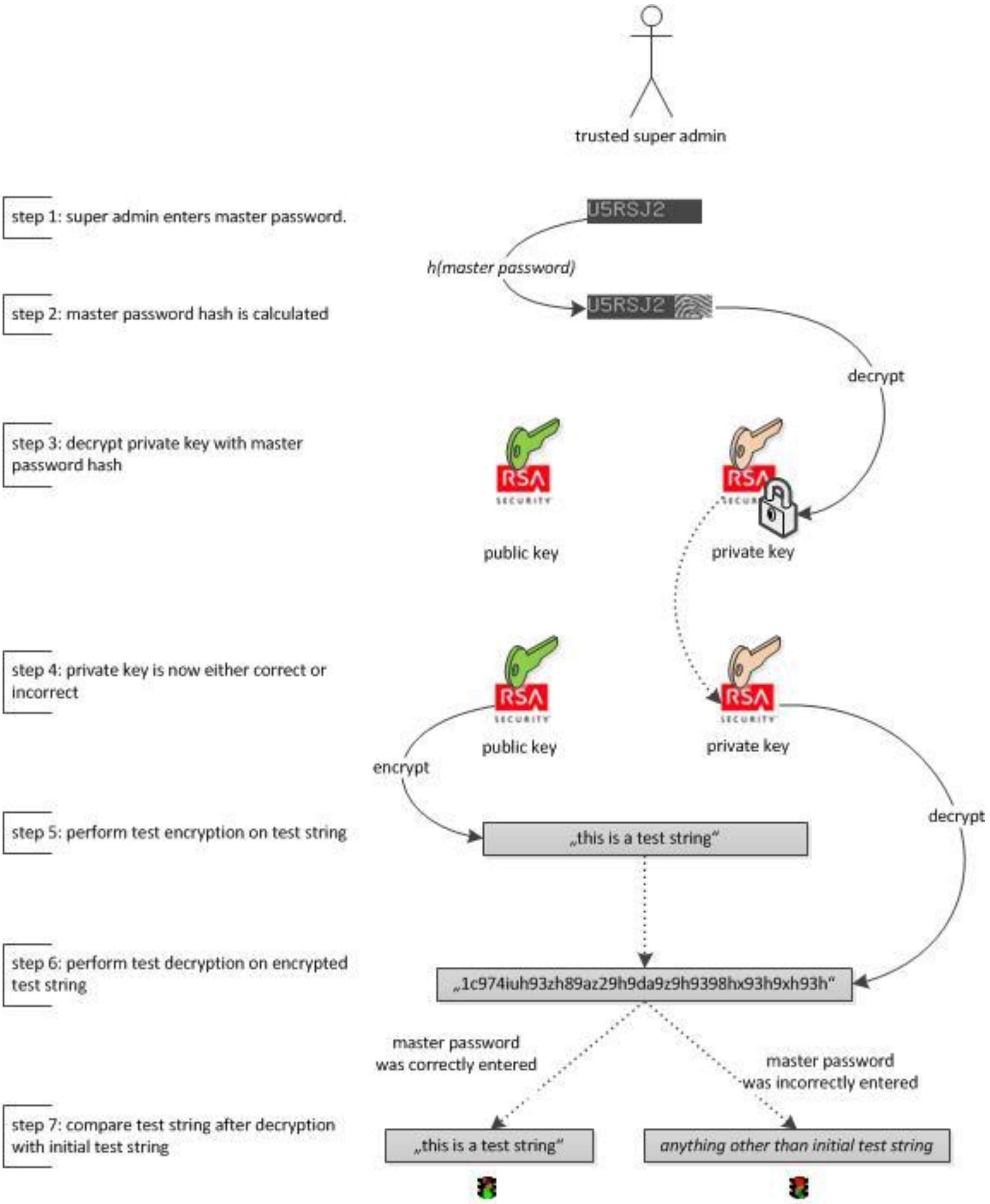

trusted super admin
step 1: super admin enters master password.
U5RSJ2
h(master password)
step 2: master password hash is calculated
U5RSJ2
decrypt
step 3: decrypt private key with master password hash
RSA SECURITY
public key
RSA SECURITY
private key
step 4: private key is now either correct or incorrect
RSA SECURITY
public key
RSA SECURITY
private key
encrypt
decrypt
step 5: perform test encryption on test string
„this is a test string“
step 6: perform test decryption on encrypted test string
„1c974iuh93zh89az29h9da9z9h9398hx93h9xh93h“
master password was correctly entered
master password was incorrectly entered
step 7: compare test string after decryption with initial test string
„this is a test string“
anything other than initial test string

Figure 21: Master password validation diagram

8.5 Search

SuD provides search functionality through the business encrypted data (clients, mandates, open issues and transactions) by using the custom Search Component. No search through encrypted documents is required.

- `Encryption Components` groups the three encryption components used for enabling the system and providing the encryption and de-encryption functionalities.

- `In-Memory Index` keeps the de-encrypted business data (clients and mandates) fields, which are stored into database as encrypted. De-encrypted data are only kept in memory.
- `Search Encryption` is the custom search components that searches through the `in-memory index` and the unencrypted data into database; and matches the search results.

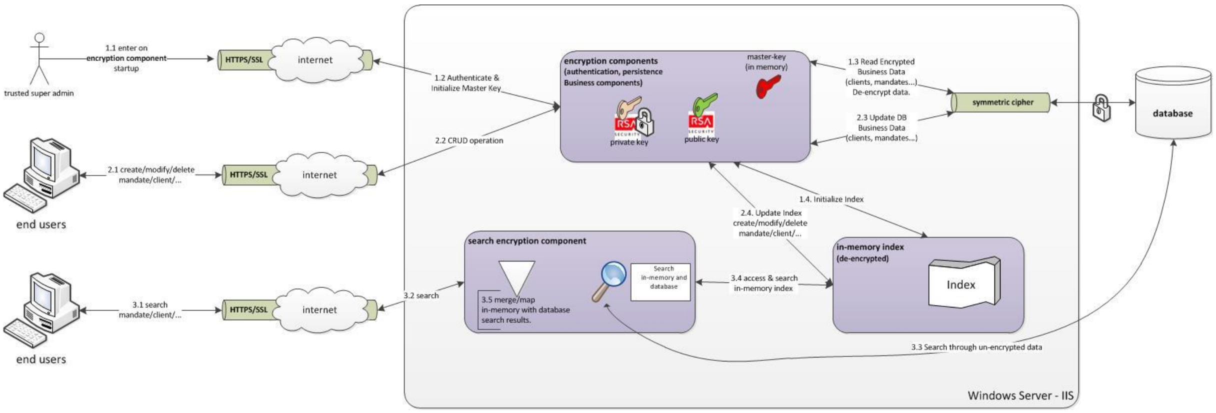


Figure 22: Search diagram

- When SuD starts/reboots (successfully authentication by the trusted-super-admin) the encryption components will prepare (read encrypted data, de-encrypt data, format data for indexing) the in-memory index.
- Any time when a client/mandate/open-issue/transaction is being created/modified/removed the in-memory index shall be updated.
- On search, the database results and in-memory results must be mapped.

9 Risks and Mitigation list

ID	Risk	Mitigation
1	An attacker successfully reaches to database server nodes and steels (reads/copies) the uploaded data (documents, business data), stored in the SuD database. Uploaded data is considered to be very secured.	All uploaded documents and sensitive information (clients, mandates, open issues and transactions) stored in the SuD database will be encrypted before saving with symmetric encryption algorithm. Data is encrypted with symmetric encryption and the keys for symmetric encryption are encrypted with asymmetric encryption algorithms. This way, attacker will not be able to decrypt and read data.
2	A SuD administrator steels (reads/copies) the database (documents, business data) and the Public & Private Keys from the "Encryption Component Persistence".	If an administrator steals the database and the Keys from the "Encryption Component Persistence" - still can't do anything, because the Public and Private Keys are protected by the "master password", which is only known by the trusted-super-admin user. The data is not compromised.
3	An attacker steels credentials of an existing user. This way, the "attacker" can log-in into SuD and see confidential data (business data and uploaded documents).	Original user contacts and requests "reset/change password" from the Active Directory administrator. An alternative would be to contact the SuD administrator who can inactivate the user account.
4	An administrator/attacker steels "master password" of trusted-super-admin user.	Original trusted-super-admin changes the "master password". Whenever the "master-password" (which is used to encrypt/de-encrypt the Public and Private key) gets changed, the data is not re-encrypted! Only the Private and Public keys are re-generated and persisted.
5	A SuD administrator is able to create memory-dumps for steeling the Master Key (kept in memory only).	The Master Key can be protected against memory dumps using the Data Protection API (.NET framework) and class SecureString. SecureStrings are text containers held in encrypted memory, and they are only unencrypted when they are accessed. The strings limit the amount of time that data is in plaintext and the memory that was used to hold an encrypted string is zeroed out when it's disposed of. So even if a memory dump is triggered, the chances are slim that valid data can be retrieved.
6	A SuD administrator steels the database, the Public & Private Keys	Another administrator tracks the SuD access (history / logs) and detects the administrator-

	and the "master password".	user and date & time of the steeling administrator.
7	SuD administrator/attacker reaches the SuD machine and reboots the system, then uses brute force attacks for "master password" cracking.	After a configurable number (5) of wrong login attempts ("master password validation"), the SuD will be blocked for a configurable number of minutes (5). With the first successful login (after block period expired) the SuD is unblocked. This blocking mechanism (for wrong login attempts) could be adopted for all type of users. A warning/alert is sent to trusted-super-admin users and administrator group.
8	The email server is not responding.	SuD sends messages to a Message Queue (persistent messages). The persisted messages are consumed by an email-delivery component which performs the sending email operation. If the mail server is not responding, the persisted message will be redelivered (after a configurable period of time) until succeeded.
9	Users upload infected (virus) files (binary content). The virus behaves in deleting accessible data (including data from file-system and database servers).	All uploaded files are scanned for viruses. If any virus is detected the data is discarded and a security message warning is sent to SuD administrator user with all details.
10	SuD database storage capacity is reached and there are new data to save.	Current storage configuration allows attaching/extending additional SSD. Extend current storage to "24 X Solid State Drive (SSD) available in 700GB".
11	All SuD database machine servers are physically destroyed because of a fire incident.	SuD has a VPN (Virtual Private Network) established with an external datacenter (different location). In order to prevent such situations, SuD is configured for disaster recovery - and backups (database dumps) are periodically (daily) saved into the datacenter. Data will be restored from these backups making the SuD available (up and running) in a very short period. It might be possible that newest data will be lost (data saved after latest backup).
12	SuD user from country A can de-encrypt/read data of users from country B - if successfully steels database and all keys.	SuD needs redesign for the Encryption Component, in order to encrypt data on country level (separate Master Key for each country).

Table 59: Risks and mitigation

10 Architecture overview

10.1 Design and Architecture Overview

SuD solution is based on the Share Point 2013 Standard Edition and .Net framework 4.x technology stack, having a multi-tier architectural solution - Service Oriented Architecture.
SuD will use the following Share Point native functionalities:

- Document management (with customized encryption component)
- Workflows
- Office Web Access provides preview of encrypted-decrypted documents and avoid traffic (read mode only - no additional license needed for read only mode; if editing will be required - additional license would be needed)
- Backup / restore - scheduler if necessary
- Audit Log to log all actions into database and keep trackiing of all users accessing the SuD
- History for documents and database records; track differences between different versions "what / who / when" - did the changes
- Security/Authentication - against Active Directory external server
- Security/Authorization - permissions at any level: documents and records (database level)
- Mail - for email notification

SuD frameworks/APIs:

- Client Tier: HTML & CSS & Java Script & JQuery - cross-browser compatibility for the most popular browsers (Mozila Firefox, Internet Explorer, Safari, Opera, Konqueror).
- Web Tier: ASP.NET
- Business Tier: C#, .Net framework 4.5 (XPath - XML search)
- Integration Tier: SharePoint CSOM / API

10.2 Design Patterns

- Inversion of Control, Dependency Injection
- Creational Design Patterns
- Behavioral Design Patterns
- Structural Design Patterns

10.3 Session Management

State of the current logged-in user is kept on the HTTP session. The user's session state is written on HTTP session immediately after success authentication and it is removed on logout (session is invalidated). No sticky sessions are used for the SuD.

10.4 Localization

~~All messages (User Interface, error messages, templates) are localized - Share Point.~~

11 Testing

11.1 Integration Tests

SuD contains integration tests specially designed for Business Tier and Presentation (web) Tier. All automatic (integration) tests run and test the correct inter-operation of multiple components accessing different business components, the database and the file system storage system (upload tests). Goals of integration testing are to verify functional, performance and reliability of designed components (considering transaction management, security, caching, database connectivity, ...). The authentication is initially performed for all tests and the security context is setup before the tests are executed. Tests require that users already exist Active Directory system (the login name and password of the test user), in order to ensure that authentication and authorization will successfully operate. Authorization is also encapsulated and tested with each integration test, based on the granted permissions and test user's role, loaded into the current user context on authentication.

11.2 Features

Depending on the project life-cycle other types of tests than the Integration Tests could be added for SuD:

- Unit tests for testing single points of classes. This should have a very well defined scope.
- Smoke tests checks if the system is up and running, testing the SuD availability.
- Regression tests for maintenance purpose. When a bug is fixed, a specific test will be implemented to ensure that the bug will not occur again.
- Acceptance tests ensure that a feature or use case is correctly implemented. It is similar to an integration test, but with a focus on the use case to provide rather than on the components involved.

11.3 Function Acceptance Tests

Functional Acceptance Tests (FAT) is based on the Test Stories from the concept. The test stage therefore is provided by TMF-Group IT, the test team consists of Itartis and SHE employees (at least 2 testers).

11.4 User Acceptance Tests

User Acceptance Test (UAT) is based on the Test Stories from the concept as well as the non-functional requirements defined in there. The tests will be performed on the future production stage and is leaded by the TMF-Group’s application owner and/or the project manager. The test team consists of selected and briefed TMF employees, project team members as well as other stakeholders (at least 4 testers).

12 Interdependencies and Interfaces

Currently the following interfaces are known.

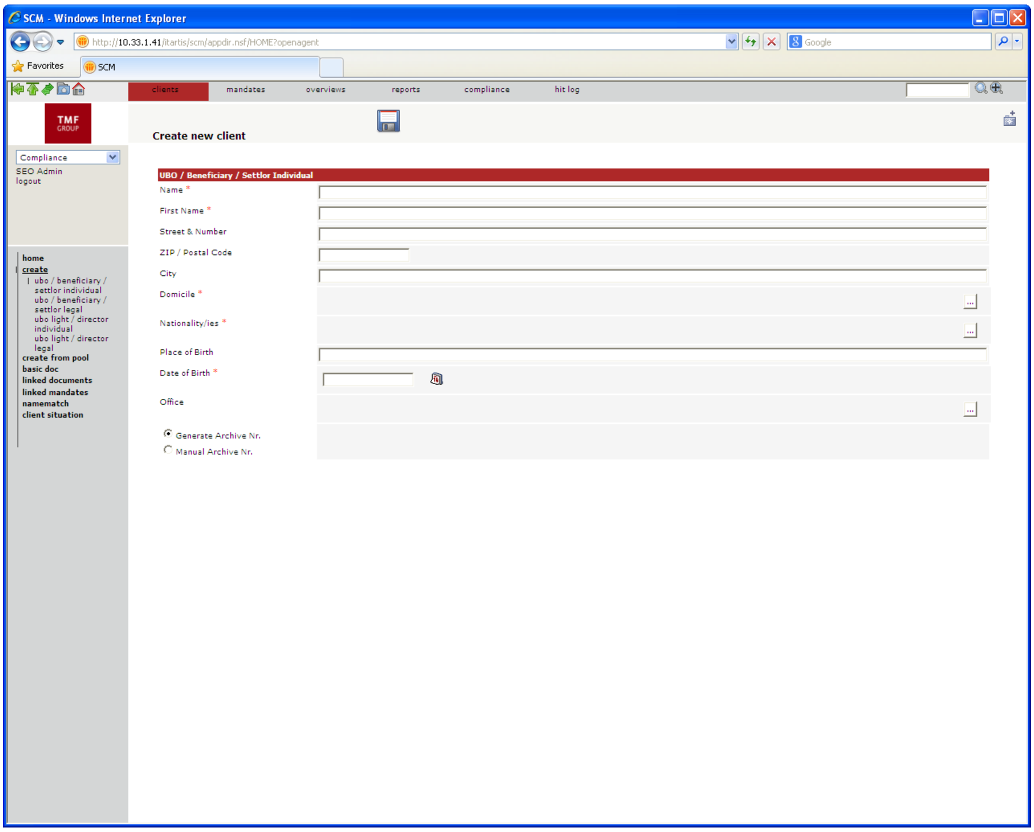
Nr.	Name	Use
1	Microsoft Active Directory	User and Group Management
2	Microsoft Office products (SharePoint Default Services)	Documents and Data exports to Spreadsheets
3	Currency and exchange rate Web service (Oanda or similar)	Currencies and exchange rates

13 Data migration

Migration of data from SEO.Old to SEO.NEXT is not part of this concept as it has to correlate with the final concept or, in this case, the further progress and findings in an agile development project.
In other words this means that the migration concept can only be defined at a later stage parallel to the construction phase of SEO.NEXT.

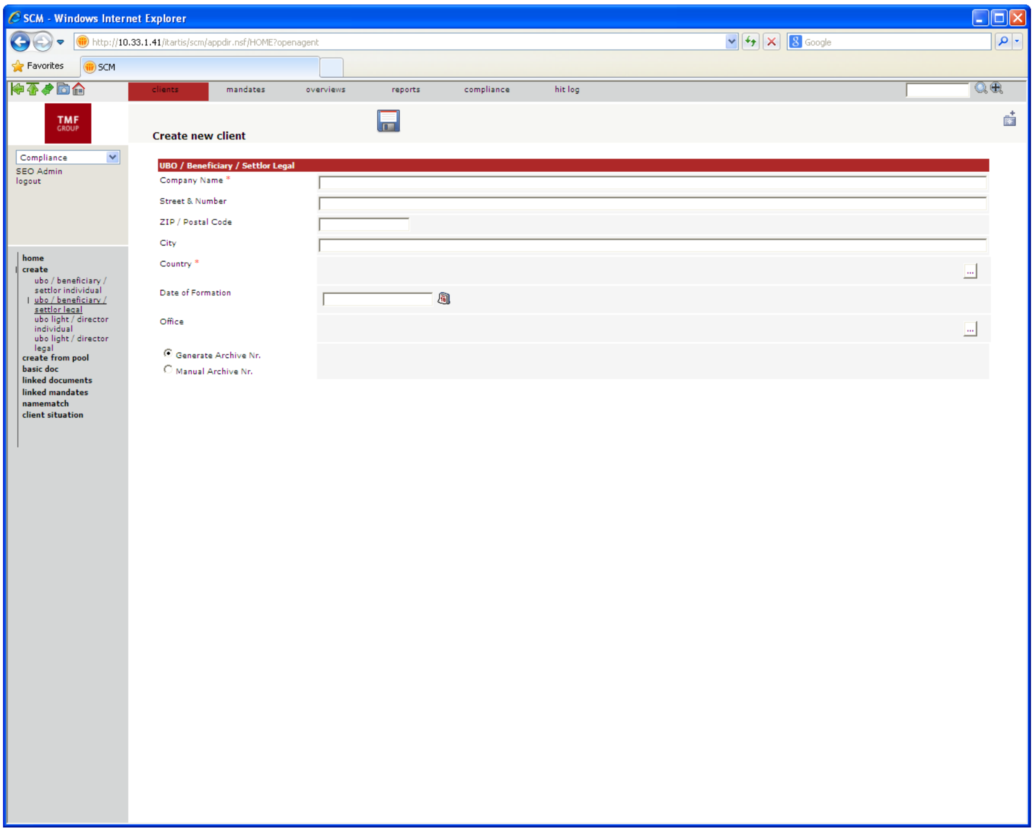
14 Appendix

14.1 Selected screenshots



● Generate Archive Nr.
○ Manual Archive Nr.

Figure 23: Create client individual



SCM - Windows Internet Explorer
http://10.33.1.41/itartis/scm/appdir.nsf/HOME?openagent
Google
Favorites
SCM
clients
mandates
overviews
reports
compliance
hit log
TMF GROUP
Compliance
SEO Admin
logout
home
create
ubo / beneficiary / settlor individual
ubo / beneficiary / settlor legal
ubo light / director individual
ubo light / director legal
create from pool
basic doc
linked documents
linked mandates
namematch
client situation

Create new client

UBO / Beneficiary / Settlor Legal

Company Name *

Street & Number

ZIP / Postal Code

City

Country *

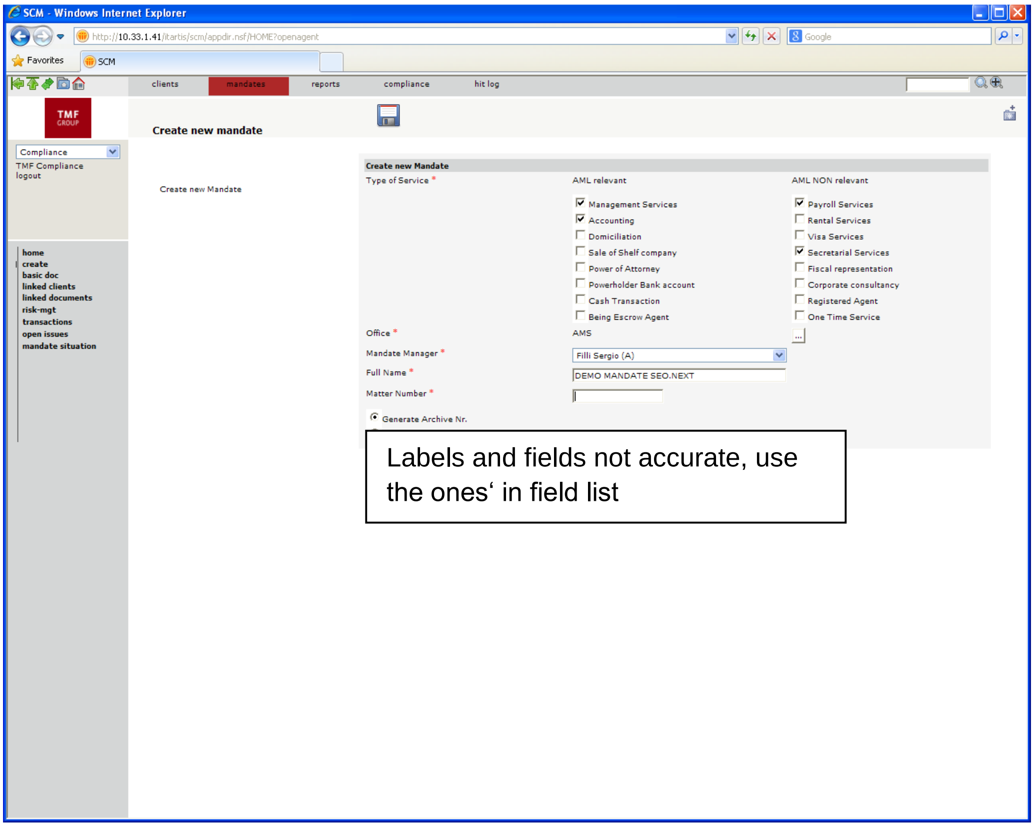
Date of Formation

Office

● Generate Archive Nr.

○ Manual Archive Nr.

Figure 24: Create client legal



Create new mandate

Create new Mandate

Create new Mandate

Type of Service *

AML relevant

☑ Management Services
☑ Accounting
☐ Domiciliation
☐ Sale of Shelf company
☐ Power of Attorney
☐ Powerholder Bank account
☐ Cash Transaction
☐ Being Escrow Agent

AML NON relevant

☑ Payroll Services
☐ Rental Services
☐ Visa Services
☑ Secretarial Services
☐ Fiscal representation
☐ Corporate consultancy
☐ Registered Agent
☐ One Time Service

Office * AMS

Mandate Manager * Filli Sergio (A)

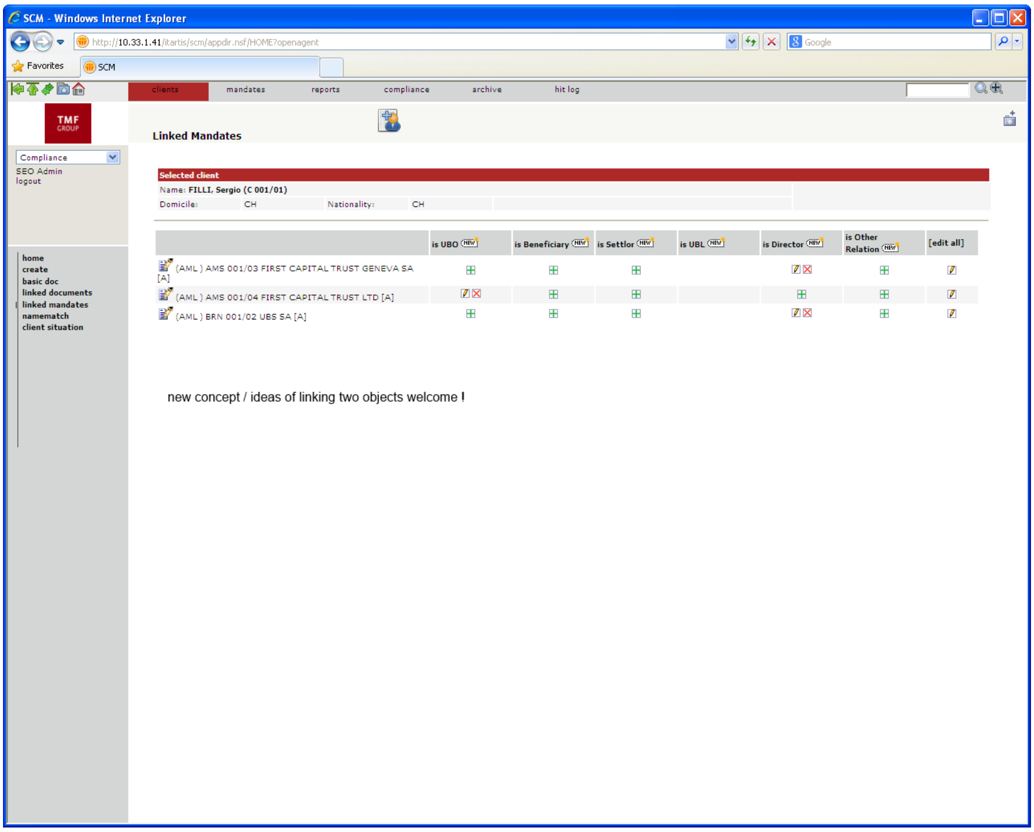
Full Name * DEMO MANDATE SEO.NEXT

Matter Number *

● Generate Archive Nr.

Labels and fields not accurate, use the ones‘ in field list

Figure 25: Create mandate



Linked Mandates

Selected client

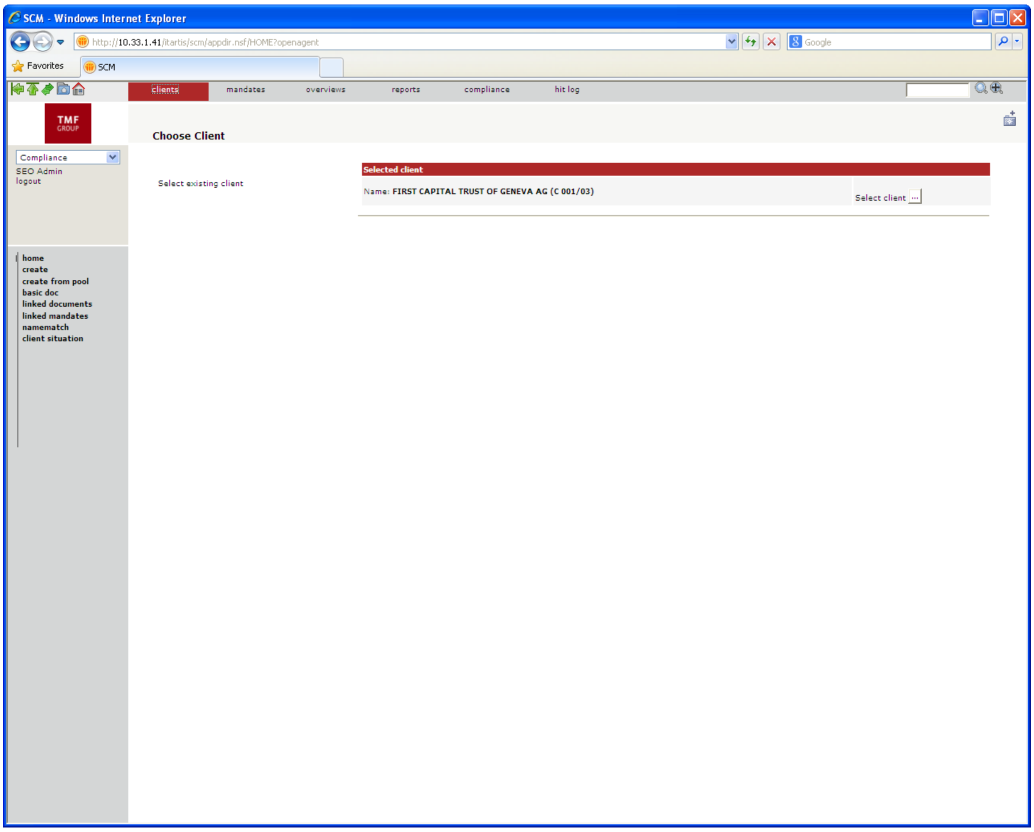
Name: **FILLI, Sergio (C 001/01)**

Domicile: CH Nationality: CH

	is UBO NEW	is Beneficiary NEW	is Settlor NEW	is UBL NEW	is Director NEW	is Other Relation NEW	[edit all]
(AML) AMS 001/03 FIRST CAPITAL TRUST GENEVA SA [A]	⊞	⊞	⊞		✎ ☒	⊞	✎
(AML) AMS 001/04 FIRST CAPITAL TRUST LTD [A]	✎ ☒	⊞	⊞		⊞	⊞	✎
(AML) BRN 001/02 UBS SA [A]	⊞	⊞	⊞		✎ ☒	⊞	✎

new concept / ideas of linking two objects welcome !

Figure 26: Create links



Choose Client

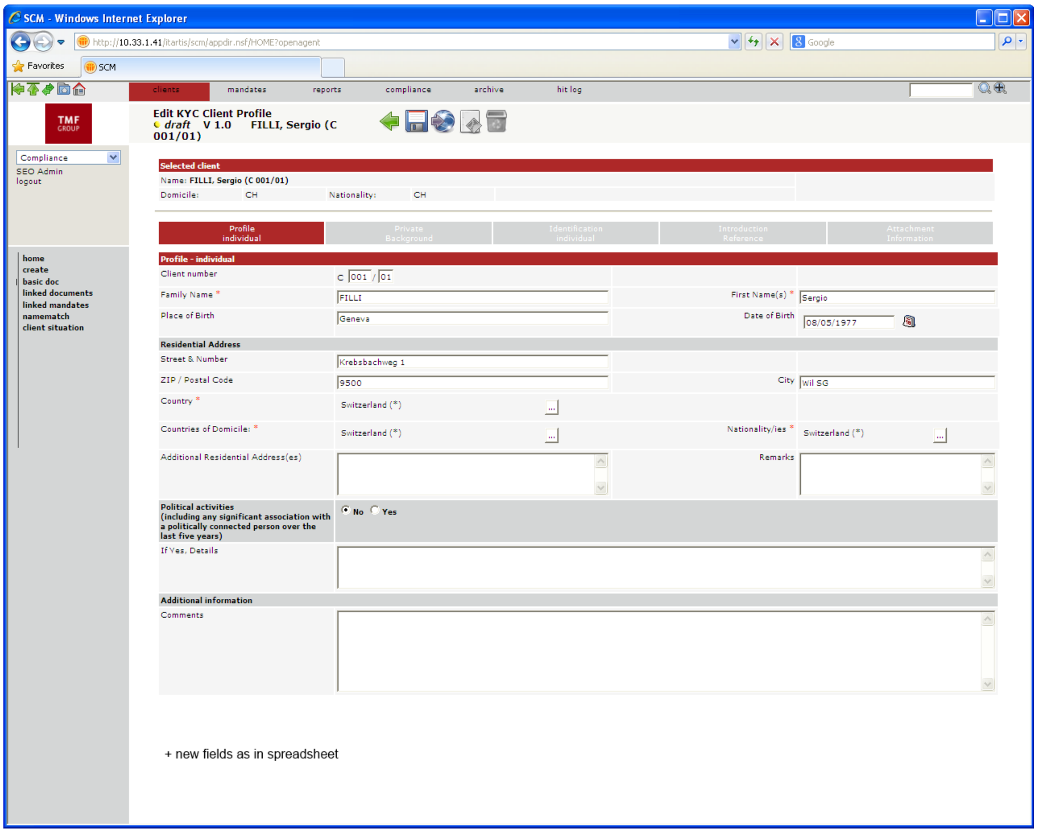
Select existing client

Selected client

Name: **FIRST CAPITAL TRUST OF GENEVA AG (C 001/03)**

Select client ...

Figure 27: Select client



Edit KYC Client Profile
draft V 1.0 FILLI, Sergio (C 001/01)

Selected client
Name: **FILLI, Sergio (C 001/01)**
Domicile: CH Nationality: CH

Profile - individual

Client number	C 001 / 01		
Family Name *	FILLI	First Name(s) *	Sergio
Place of Birth	Geneva	Date of Birth	08/05/1977

Residential Address

Street & Number	Krebsbachweg 1		
ZIP / Postal Code	9500	City	Wil SG
Country *	Switzerland (*) ...		
Countries of Domicile: *	Switzerland (*) ...	Nationality/ies *	Switzerland (*) ...
Additional Residential Address(es)		Remarks	

Political activities
(including any significant association with a politically connected person over the last five years) ● No ○ Yes

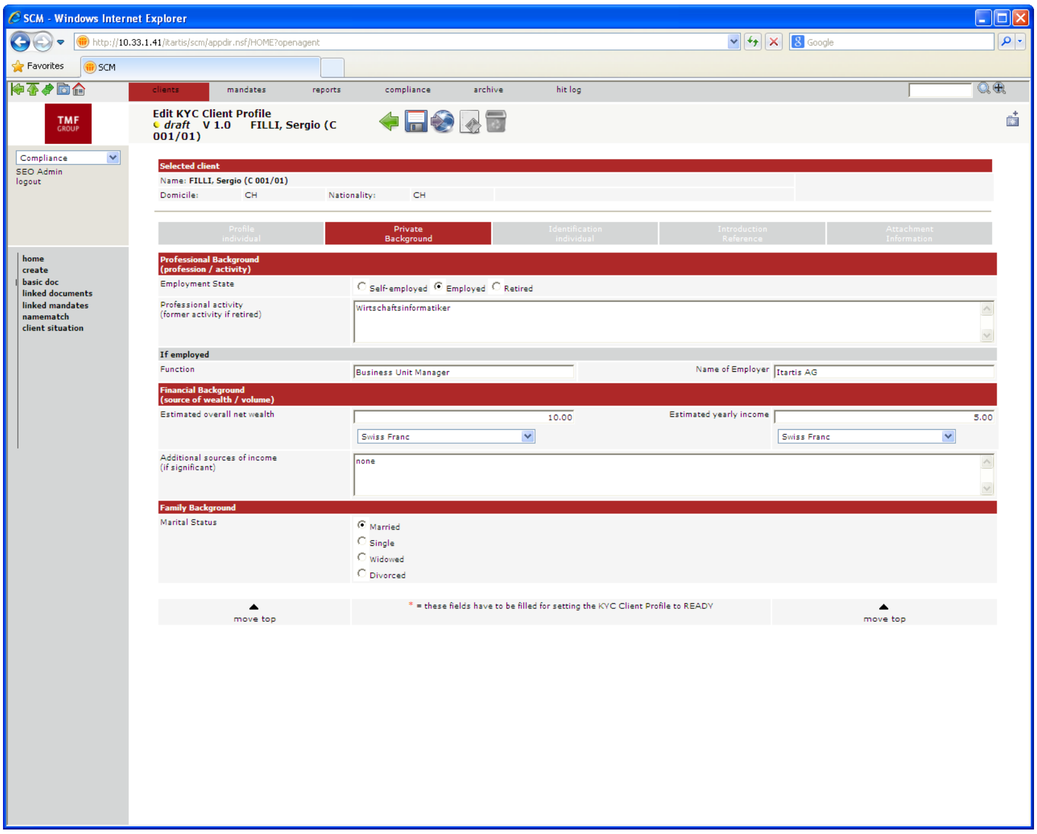
If Yes, Details

Additional information

Comments

+ new fields as in spreadsheet

Figure 28: Basic doc client individual - profile tab



Edit KYC Client Profile
draft V 1.0 FILLI, Sergio (C 001/01)

Selected client
Name: **FILLI, Sergio (C 001/01)**
Domicile: CH Nationality: CH

Professional Background (profession / activity)

Employment State	○ Self-employed ● Employed ○ Retired		
Professional activity (former activity if retired)	Wirtschaftsinformatiker		

If employed

Function	Business Unit Manager	Name of Employer	Itartis AG

Financial Background (source of wealth / volume)

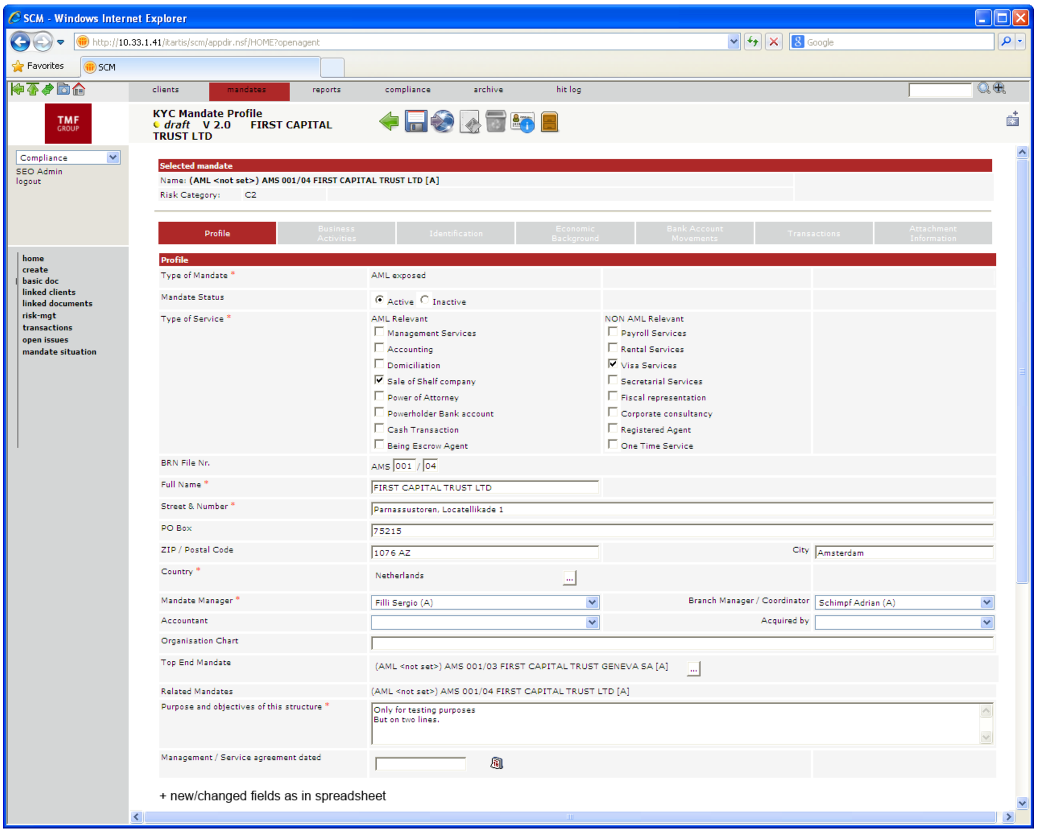
Estimated overall net wealth	10.00 Swiss Franc	Estimated yearly income	5.00 Swiss Franc
Additional sources of income (if significant)	none		

Family Background

Marital Status
● Married
○ Single
○ Widowed
○ Divorced

* = these fields have to be filled for setting the KYC Client Profile to READY

Figure 29: Basic doc client individual - professional background tab



KYC Mandate Profile
draft V 2.0 FIRST CAPITAL TRUST LTD

Selected mandate

Name: **(AML <not set>) AMS 001/04 FIRST CAPITAL TRUST LTD [A]**

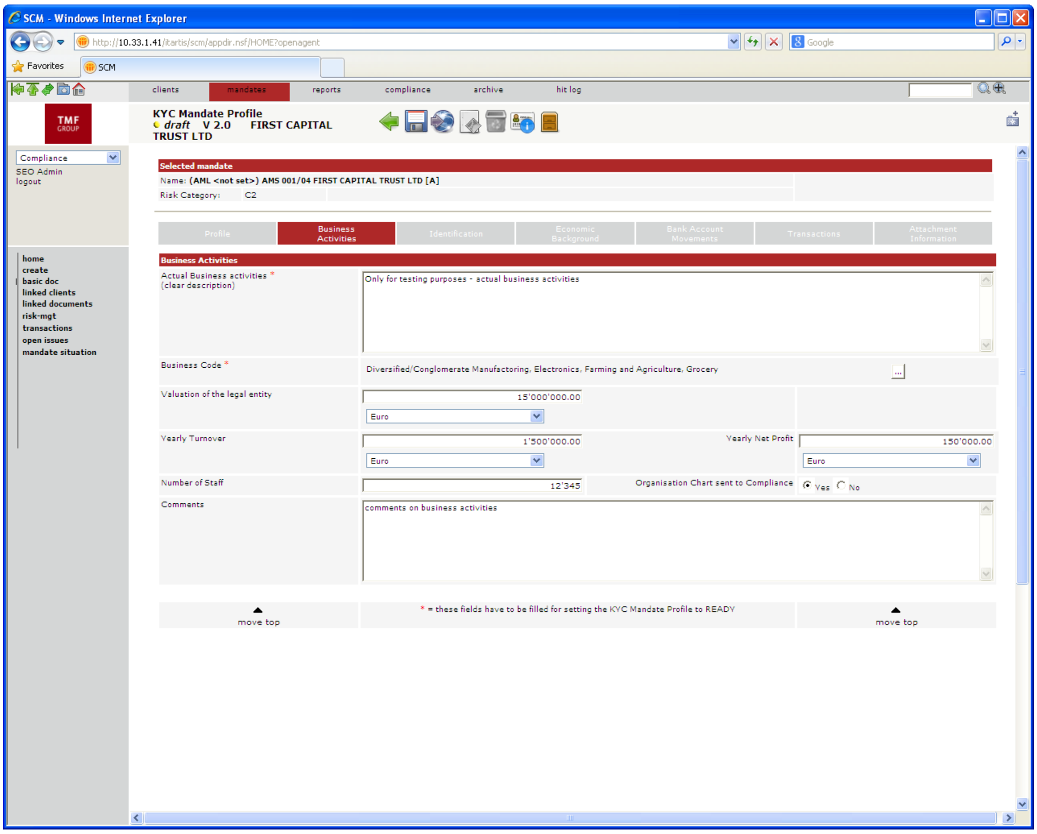
Risk Category: C2

Profile

Type of Mandate *	AML exposed		
Mandate Status	● Active ○ Inactive		
Type of Service *	AML Relevant □ Management Services □ Accounting □ Domiciliation ☑ Sale of Shelf company □ Power of Attorney □ Powerholder Bank account □ Cash Transaction □ Being Escrow Agent	NON AML Relevant □ Payroll Services □ Rental Services ☑ Visa Services □ Secretarial Services □ Fiscal representation □ Corporate consultancy □ Registered Agent □ One Time Service	
BRN File Nr.	AMS 001 / 04		
Full Name *	FIRST CAPITAL TRUST LTD		
Street & Number *	Parnassustoren, Locatellikade 1		
PO Box	75215		
ZIP / Postal Code	1076 AZ	City	Amsterdam
Country *	Netherlands ...		
Mandate Manager *	Filli Sergio (A)	Branch Manager / Coordinator	Schimpf Adrian (A)
Accountant		Acquired by	
Organisation Chart			
Top End Mandate	(AML <not set>) AMS 001/03 FIRST CAPITAL TRUST GENEVA SA [A] ...		
Related Mandates	(AML <not set>) AMS 001/04 FIRST CAPITAL TRUST LTD [A]		
Purpose and objectives of this structure *	Only for testing purposes But on two lines.		
Management / Service agreement dated			

+ new/changed fields as in spreadsheet

Figure 30: Basic doc mandate - profile tab



KYC Mandate Profile
draft V 2.0 FIRST CAPITAL TRUST LTD

Selected mandate

Name: **(AML <not set>) AMS 001/04 FIRST CAPITAL TRUST LTD [A]**

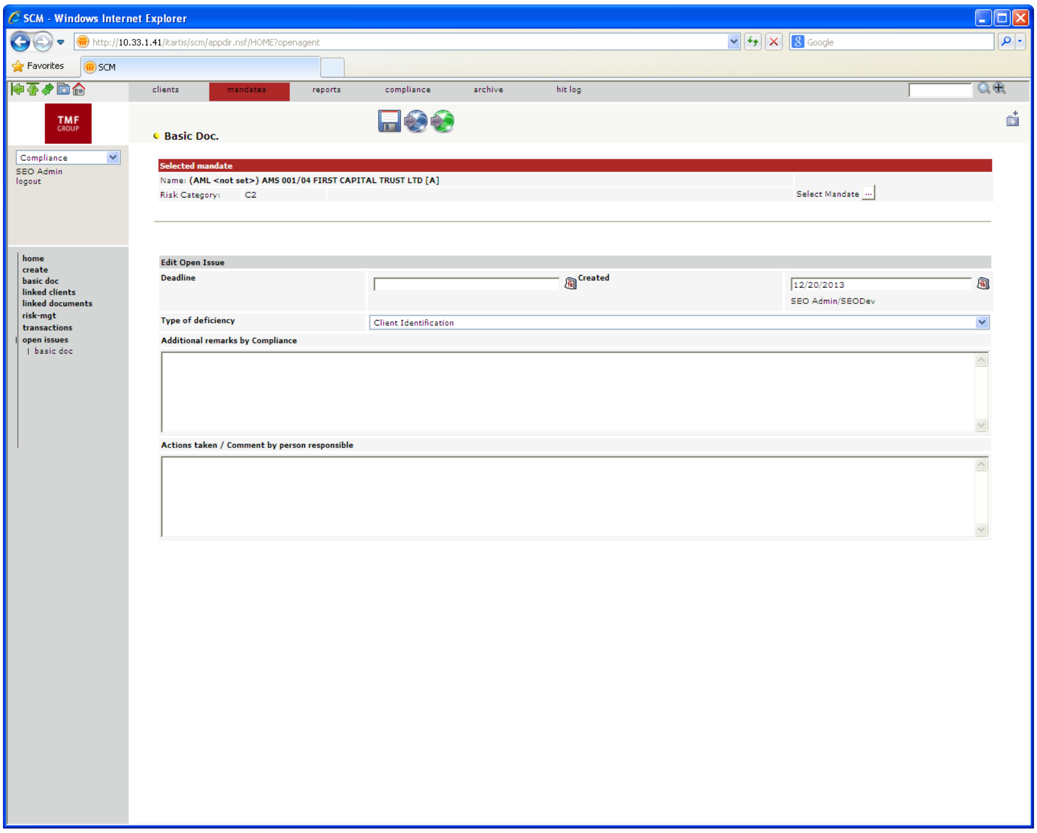
Risk Category: C2

Business Activities

Actual Business activities * (clear description)	Only for testing purposes - actual business activities		
Business Code *	Diversified/Conglomerate Manufactoring, Electronics, Farming and Agriculture, Grocery ...		
Valuation of the legal entity	15'000'000.00 Euro		
Yearly Turnover	1'500'000.00 Euro	Yearly Net Profit	150'000.00 Euro
Number of Staff	12'345	Organisation Chart sent to Compliance	● Yes ○ No
Comments	comments on business activities		

* = these fields have to be filled for setting the KYC Mandate Profile to READY

Figure 31: Basic doc mandate - business activities tab



Basic Doc.

Selected mandate

Name: (AML <not set>) AMS 001/04 FIRST CAPITAL TRUST LTD [A]

Risk Category: C2

Edit Open Issue

Deadline

Created 12/20/2013

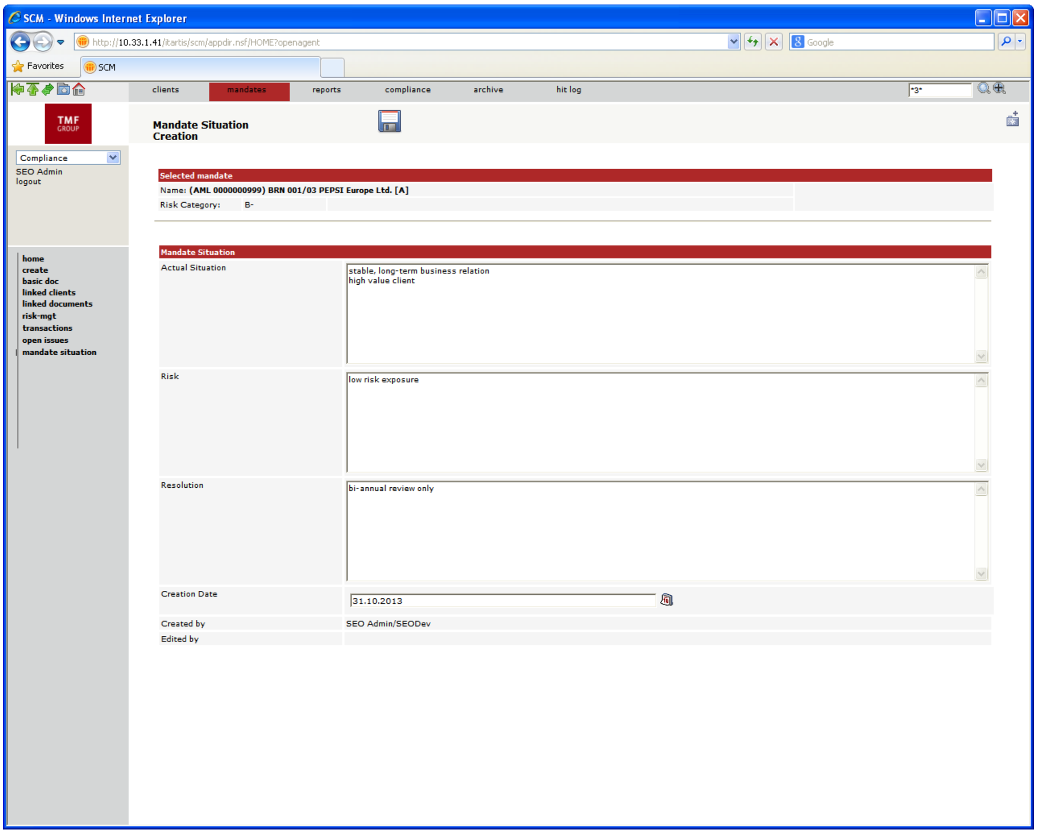
SEO Admin/SEODev

Type of deficiency: Client Identification

Additional remarks by Compliance

Actions taken / Comment by person responsible

Figure 32: Create open issue - type basic doc



Mandate Situation Creation

Selected mandate

Name: (AML 0000000999) BRN 001/03 PEPSI Europe Ltd. [A]

Risk Category: B-

Mandate Situation

Actual Situation: stable, long-term business relation
high value client

Risk: low risk exposure

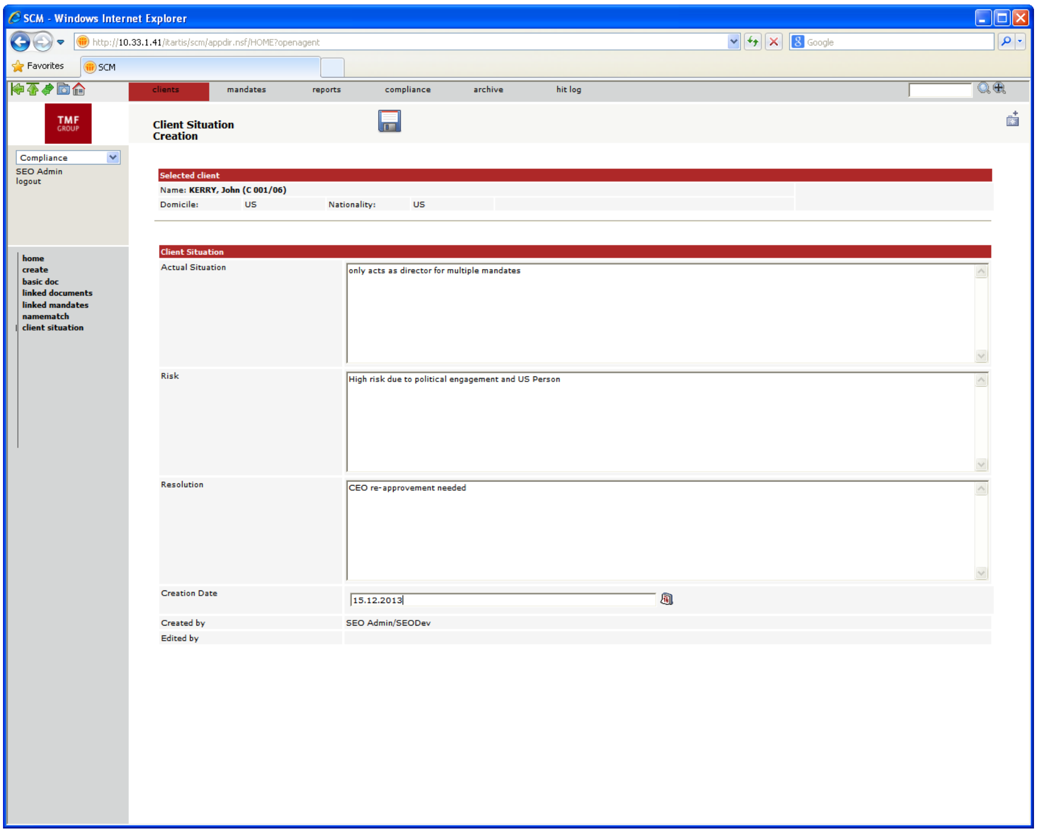
Resolution: bi-annual review only

Creation Date: 31.10.2013

Created by: SEO Admin/SEODev

Edited by

Figure 33: Create mandate situation



Client Situation Creation

Selected client

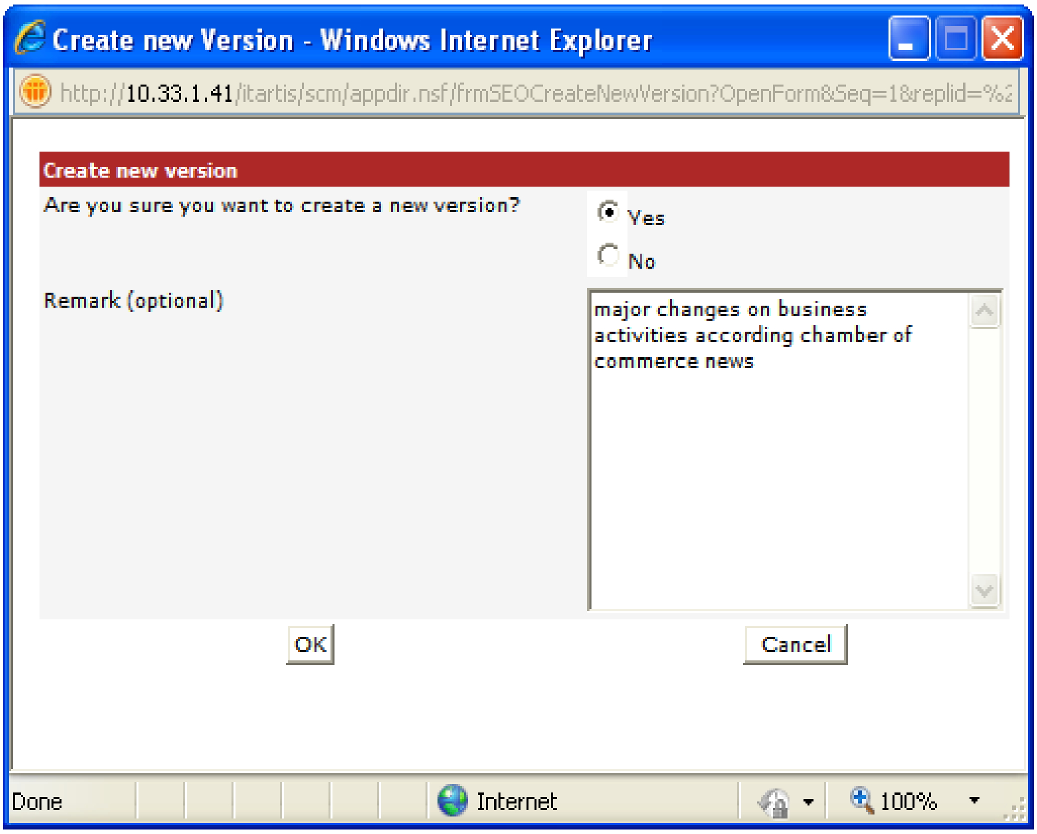
Name: **KERRY, John (C 001/06)**

Domicile: US Nationality: US

Client Situation

Actual Situation	only acts as director for multiple mandates
Risk	High risk due to political engagement and US Person
Resolution	CEO re-approvement needed
Creation Date	15.12.2013
Created by	SEO Admin/SEODev
Edited by	

Figure 34: Create client situation

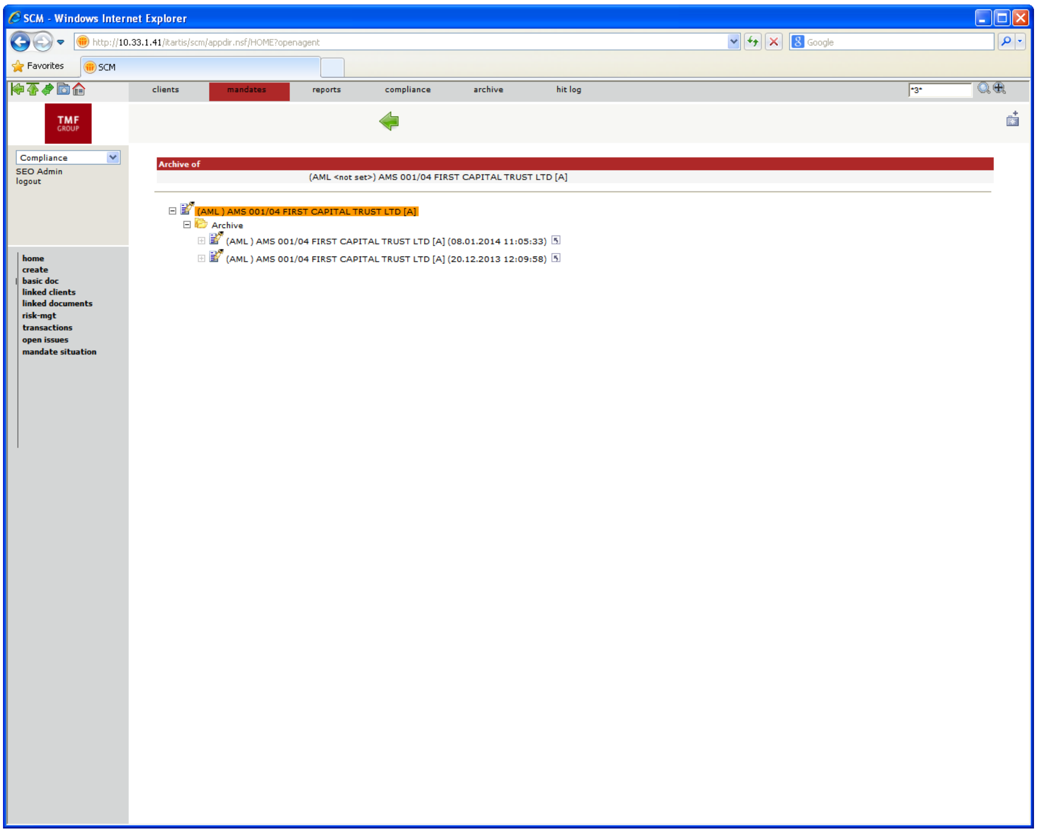

Create new Version - Windows Internet Explorer
http://10.33.1.41/itartis/scm/appdir.nsf/frmSEOCreateNewVersion?OpenForm&Seq=1&replid=%2
OK
Cancel
Done
Internet
100%

Create new version

Are you sure you want to create a new version? ● Yes ○ No

Remark (optional): major changes on business activities according chamber of commerce news

Figure 35: New version dialog windows

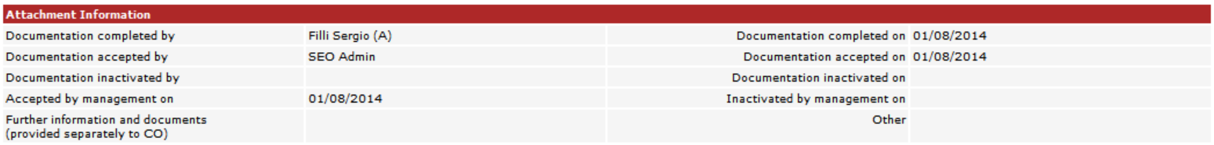


Archive of

(AML <not set>) AMS 001/04 FIRST CAPITAL TRUST LTD [A]

- (AML) AMS 001/04 FIRST CAPITAL TRUST LTD [A]
  - Archive
    - (AML) AMS 001/04 FIRST CAPITAL TRUST LTD [A] (08.01.2014 11:05:33)
    - (AML) AMS 001/04 FIRST CAPITAL TRUST LTD [A] (20.12.2013 12:09:58)

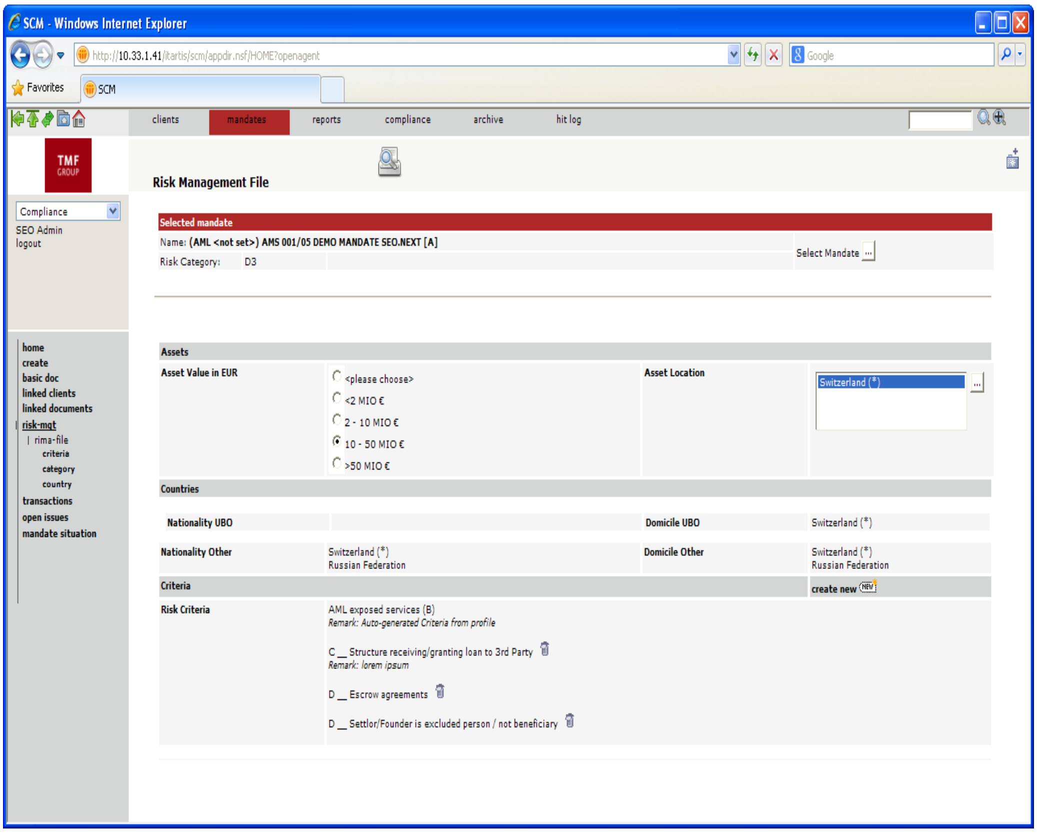
Figure 36: Mandate archive overview



Attachment Information

Documentation completed by	Filli Sergio (A)	Documentation completed on	01/08/2014
Documentation accepted by	SEO Admin	Documentation accepted on	01/08/2014
Documentation inactivated by		Documentation inactivated on	
Accepted by management on	01/08/2014	Inactivated by management on	
Further information and documents (provided separately to CO)		Other	

Figure 37: Workflow fields in basic doc



Risk Management File

Selected mandate

Name: **(AML <not set>) AMS 001/05 DEMO MANDATE SEO.NEXT [A]**

Risk Category: D3

Select Mandate ...

Assets

Asset Value in EUR

○ <please choose>
○ <2 MIO €
○ 2 - 10 MIO €
● 10 - 50 MIO €
○ >50 MIO €

Asset Location

Switzerland (*)

Countries

Nationality UBO		**Domicile UBO**	Switzerland (*)
Nationality Other	Switzerland (*) Russian Federation	**Domicile Other**	Switzerland (*) Russian Federation

Criteria — **create new**

Risk Criteria

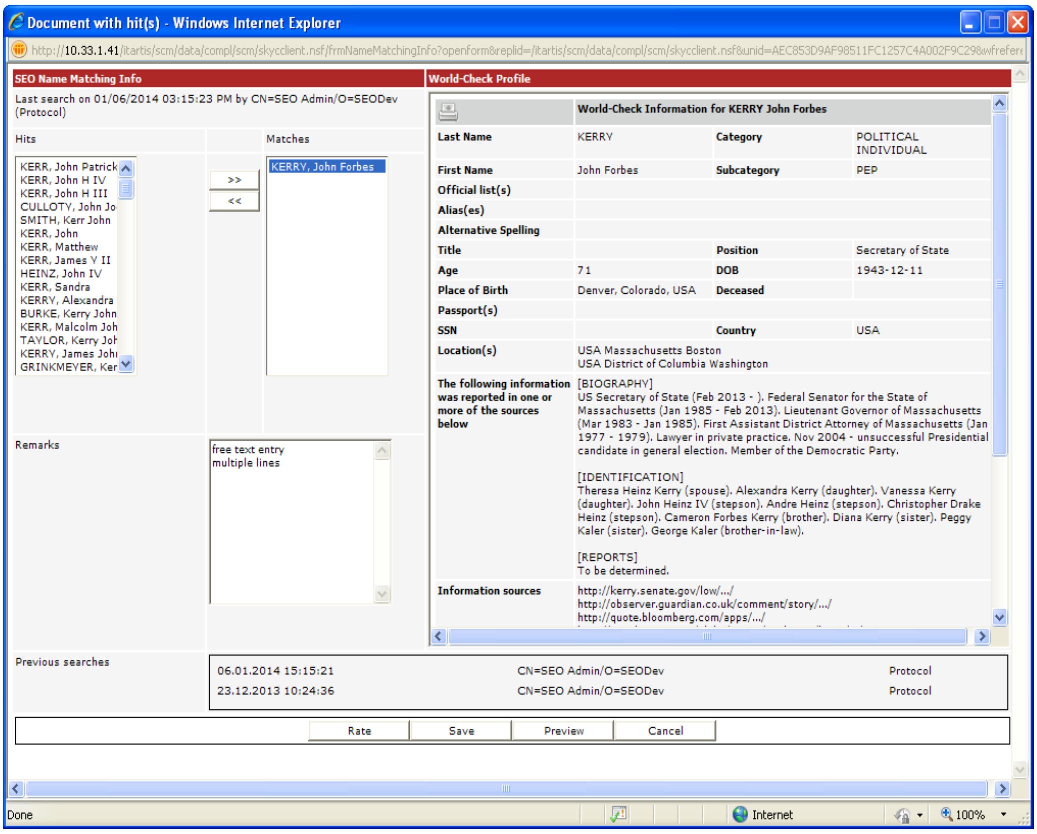
AML exposed services (B)
Remark: Auto-generated Criteria from profile

C __ Structure receiving/granting loan to 3rd Party
Remark: lorem ipsum

D __ Escrow agreements

D __ Settlor/Founder is excluded person / not beneficiary

Figure 38: Risk profile


Document with hit(s) - Windows Internet Explorer
http://10.33.1.41/itartis/scm/data/compl/scm/skycclient.nsf/frmNameMatchingInfo?openform&replid=/itartis/scm/data/compl/scm/skycclient.nsf&unid=AEC853D9AF98511FC1257C4A002F9C29&wfrefere
>>
<<
Rate
Save
Preview
Cancel
Done
Internet
100%

SEO Name Matching Info

Last search on 01/06/2014 03:15:23 PM by CN=SEO Admin/O=SEODev (Protocol)

Hits

KERR, John Patrick
KERR, John H IV
KERR, John H III
CULLOTY, John Jo
SMITH, Kerr John
KERR, John
KERR, Matthew
KERR, James Y II
HEINZ, John IV
KERR, Sandra
KERRY, Alexandra
BURKE, Kerry John
KERR, Malcolm Joh
TAYLOR, Kerry Joh
KERRY, James Johi
GRINKMEYER, Ker

Matches

KERRY, John Forbes

Remarks

free text entry
multiple lines

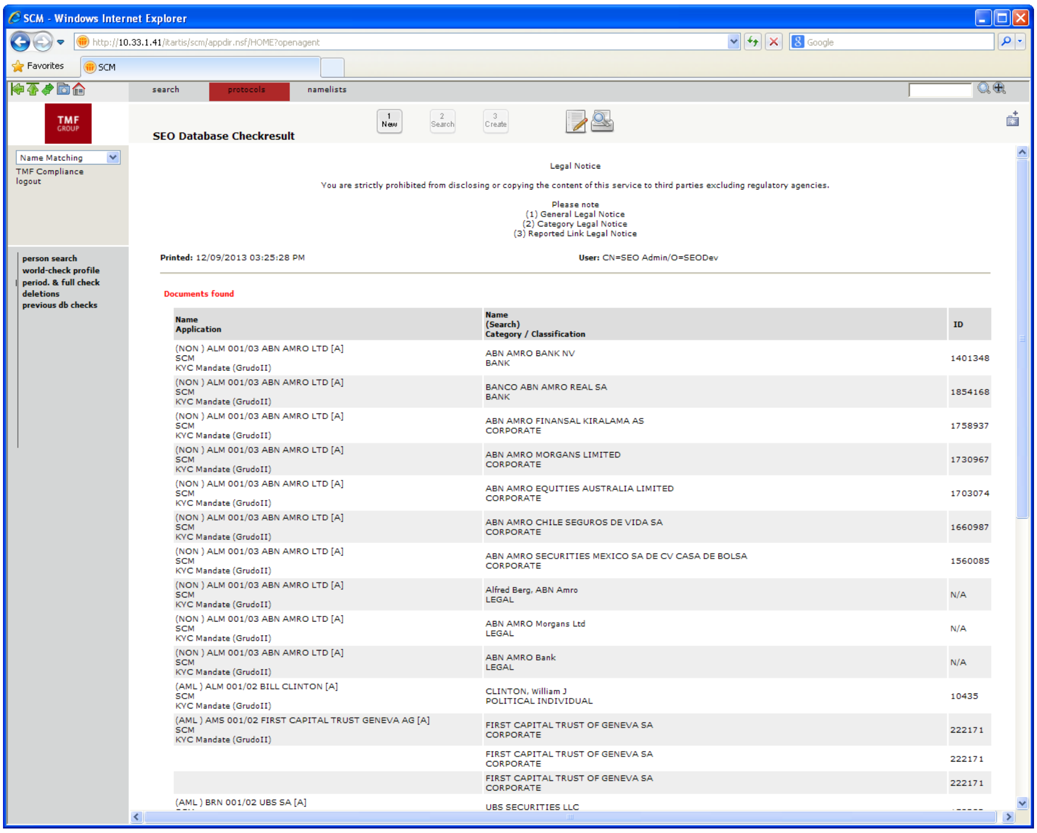
Previous searches

06.01.2014 15:15:21	CN=SEO Admin/O=SEODev	Protocol
23.12.2013 10:24:36	CN=SEO Admin/O=SEODev	Protocol

World-Check Profile

	World-Check Information for KERRY John Forbes		
Last Name	KERRY	**Category**	POLITICAL INDIVIDUAL
First Name	John Forbes	**Subcategory**	PEP
Official list(s)			
Alias(es)			
Alternative Spelling			
Title		**Position**	Secretary of State
Age	71	**DOB**	1943-12-11
Place of Birth	Denver, Colorado, USA	**Deceased**	
Passport(s)			
SSN		**Country**	USA
Location(s)	USA Massachusetts Boston USA District of Columbia Washington		
The following information was reported in one or more of the sources below	[BIOGRAPHY] US Secretary of State (Feb 2013 -). Federal Senator for the State of Massachusetts (Jan 1985 - Feb 2013). Lieutenant Governor of Massachusetts (Mar 1983 - Jan 1985). First Assistant District Attorney of Massachusetts (Jan 1977 - 1979). Lawyer in private practice. Nov 2004 - unsuccessful Presidential candidate in general election. Member of the Democratic Party. [IDENTIFICATION] Theresa Heinz Kerry (spouse). Alexandra Kerry (daughter). Vanessa Kerry (daughter). John Heinz IV (stepson). Andre Heinz (stepson). Christopher Drake Heinz (stepson). Cameron Forbes Kerry (brother). Diana Kerry (sister). Peggy Kaler (sister). George Kaler (brother-in-law). [REPORTS] To be determined.		
Information sources	http://kerry.senate.gov/low/.../ http://observer.guardian.co.uk/comment/story/.../ http://quote.bloomberg.com/apps/.../		

Figure 39: Name Matching Rating



SEO Database Checkresult

Legal Notice

You are strictly prohibited from disclosing or copying the content of this service to third parties excluding regulatory agencies.

Please note
(1) General Legal Notice
(2) Category Legal Notice
(3) Reported Link Legal Notice

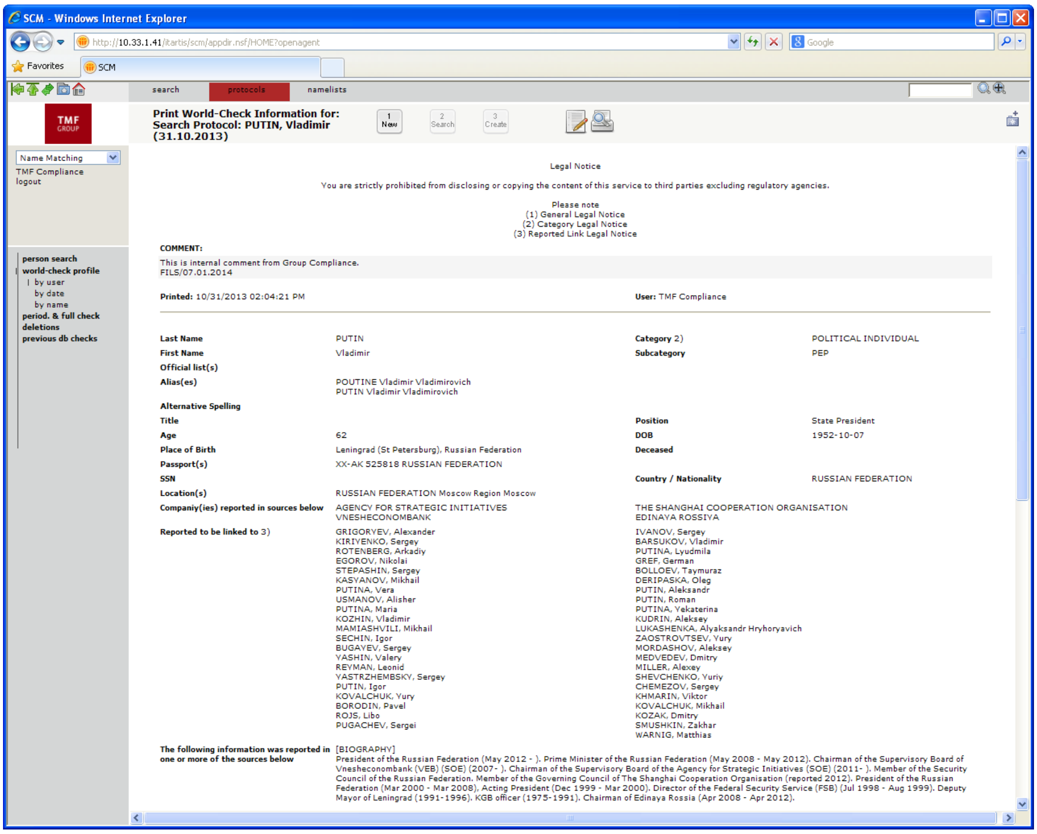
Printed: 12/09/2013 03:25:28 PM

User: CN=SEO Admin/O=SEODev

Documents found

Name Application	Name (Search) Category / Classification	ID
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO BANK NV BANK	1401348
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	BANCO ABN AMRO REAL SA BANK	1854168
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO FINANSAL KIRALAMA AS CORPORATE	1758937
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO MORGANS LIMITED CORPORATE	1730967
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO EQUITIES AUSTRALIA LIMITED CORPORATE	1703074
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO CHILE SEGUROS DE VIDA SA CORPORATE	1660987
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO SECURITIES MEXICO SA DE CV CASA DE BOLSA CORPORATE	1560085
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	Alfred Berg, ABN Amro LEGAL	N/A
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO Morgans Ltd LEGAL	N/A
(NON) ALM 001/03 ABN AMRO LTD [A] SCM KYC Mandate (GrudoII)	ABN AMRO Bank LEGAL	N/A
(AML) ALM 001/02 BILL CLINTON [A] SCM KYC Mandate (GrudoII)	CLINTON, William J POLITICAL INDIVIDUAL	10435
(AML) AMS 001/02 FIRST CAPITAL TRUST GENEVA AG [A] SCM KYC Mandate (GrudoII)	FIRST CAPITAL TRUST OF GENEVA SA CORPORATE	222171
	FIRST CAPITAL TRUST OF GENEVA SA CORPORATE	222171
	FIRST CAPITAL TRUST OF GENEVA SA CORPORATE	222171
(AML) BRN 001/02 UBS SA [A]	UBS SECURITIES LLC	

Figure 40: Name Matching Check Protocol



**Print World-Check Information for:
Search Protocol: PUTIN, Vladimir
(31.10.2013)**

Legal Notice

You are strictly prohibited from disclosing or copying the content of this service to third parties excluding regulatory agencies.

Please note
(1) General Legal Notice
(2) Category Legal Notice
(3) Reported Link Legal Notice

COMMENT:

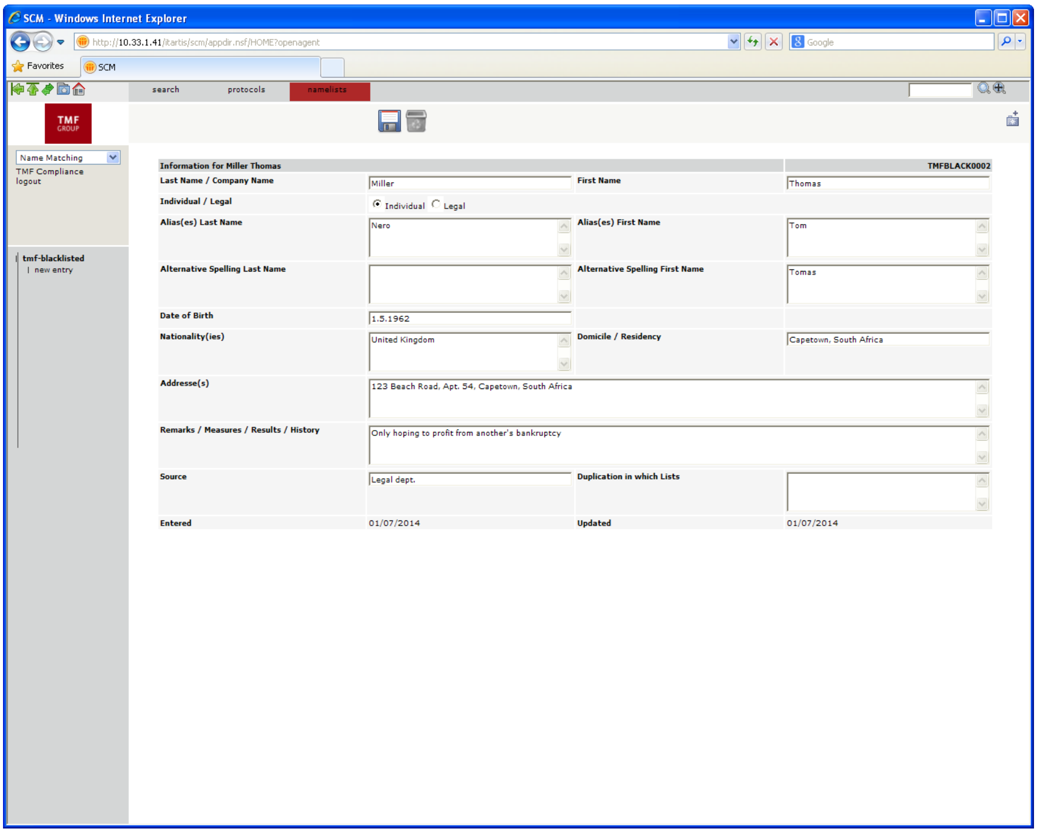
This is internal comment from Group Compliance.
FILS/07.01.2014

Printed: 10/31/2013 02:04:21 PM

User: TMF Compliance

Last Name	PUTIN	**Category** 2)	POLITICAL INDIVIDUAL
First Name	Vladimir	**Subcategory**	PEP
Official list(s)			
Alias(es)	POUTINE Vladimir Vladimirovich PUTIN Vladimir Vladimirovich		
Alternative Spelling			
Title		**Position**	State President
Age	62	**DOB**	1952-10-07
Place of Birth	Leningrad (St Petersburg), Russian Federation	**Deceased**	
Passport(s)	XX-AK 525818 RUSSIAN FEDERATION		
SSN		**Country / Nationality**	RUSSIAN FEDERATION
Location(s)	RUSSIAN FEDERATION Moscow Region Moscow		
Companiy(ies) reported in sources below	AGENCY FOR STRATEGIC INITIATIVES VNESHECONOMBANK	THE SHANGHAI COOPERATION ORGANISATION EDINAYA ROSSIYA	
Reported to be linked to 3)	GRIGORYEV, Alexander KIRIYENKO, Sergey ROTENBERG, Arkadiy EGOROV, Nikolai STEPASHIN, Sergey KASYANOV, Mikhail PUTINA, Vera USMANOV, Alisher PUTINA, Maria KOZHIN, Vladimir MAMIASHVILI, Mikhail SECHIN, Igor BUGAYEV, Sergey YASHIN, Valery REYMAN, Leonid YASTRZHEMBSKY, Sergey PUTIN, Igor KOVALCHUK, Yury BORODIN, Pavel ROJS, Libo PUGACHEV, Sergei	IVANOV, Sergey BARSUKOV, Vladimir PUTINA, Lyudmila GREF, German BOLLOEV, Taymuraz DERIPASKA, Oleg PUTIN, Aleksandr PUTIN, Roman PUTINA, Yekaterina KUDRIN, Aleksey LUKASHENKA, Alyaksandr Hryhoryavich ZAOSTROVTSEV, Yury MORDASHOV, Aleksey MEDVEDEV, Dmitry MILLER, Alexey SHEVCHENKO, Yuriy CHEMEZOV, Sergey KHMARIN, Viktor KOVALCHUK, Mikhail KOZAK, Dmitry SMUSHKIN, Zakhar WARNIG, Matthias	
The following information was reported in one or more of the sources below	[BIOGRAPHY] President of the Russian Federation (May 2012 -). Prime Minister of the Russian Federation (May 2008 - May 2012). Chairman of the Supervisory Board of Vnesheconombank (VEB) (SOE) (2007-). Chairman of the Supervisory Board of the Agency for Strategic Initiatives (SOE) (2011-). Member of the Security Council of the Russian Federation. Member of the Governing Council of The Shanghai Cooperation Organisation (reported 2012). President of the Russian Federation (Mar 2000 - Mar 2008), Acting President (Dec 1999 - Mar 2000). Director of the Federal Security Service (FSB) (Jul 1998 - Aug 1999). Deputy Mayor of Leningrad (1991-1996). KGB officer (1975-1991). Chairman of Edinaya Rossia (Apr 2008 - Apr 2012).		

Figure 41: World-Check Protocol



Information for Miller Thomas			TMFBLACK0002
Last Name / Company Name	Miller	First Name	Thomas
Individual / Legal	● Individual ○ Legal		
Alias(es) Last Name	Nero	Alias(es) First Name	Tom
Alternative Spelling Last Name		Alternative Spelling First Name	Tomas
Date of Birth	1.5.1962		
Nationality(ies)	United Kingdom	Domicile / Residency	Capetown, South Africa
Addresse(s)	123 Beach Road, Apt. 54, Capetown, South Africa		
Remarks / Measures / Results / History	Only hoping to profit from another's bankruptcy		
Source	Legal dept.	Duplication in which Lists	
Entered	01/07/2014	Updated	01/07/2014

Figure 42: Blacklist Entry

14.2 Status flow diagrams

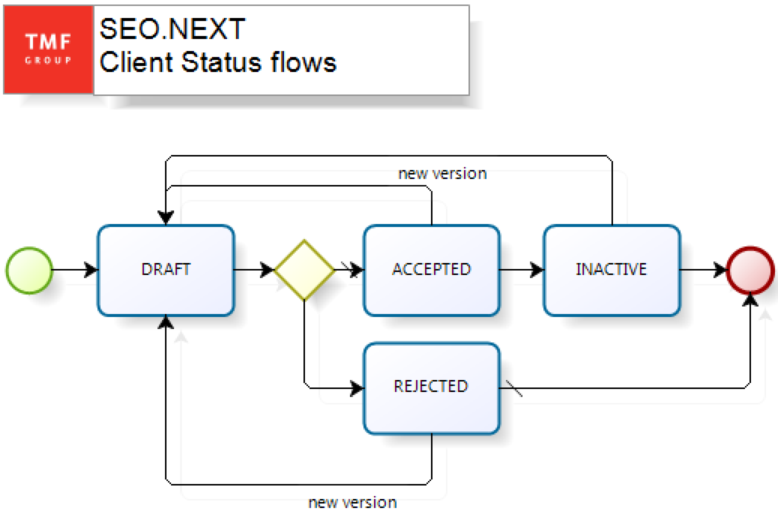


Figure 43: Client status flow

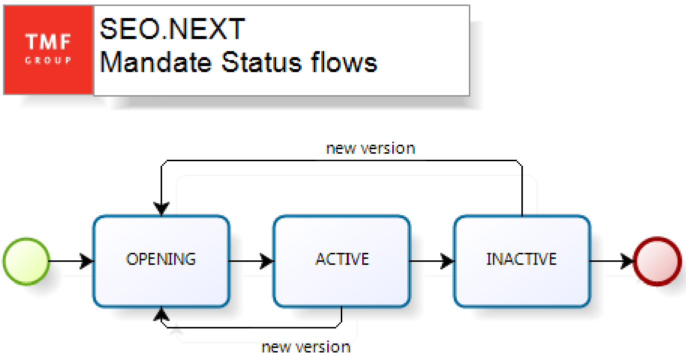


Figure 44: Mandate Status flows

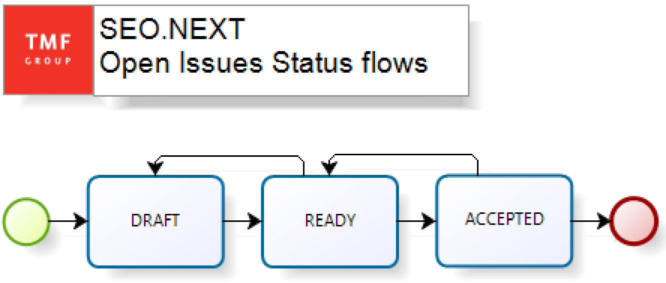


Figure 45: Open Issues Status flows

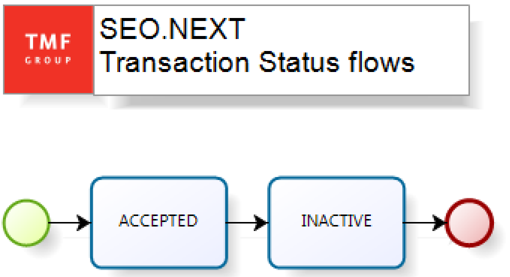


Figure 46: Transaction Status flows

Document information

Approval

	Date	Name	Signature
Author	06.12.2013	Sergio Filli	
Approved by Itartis			
Approved by CLIENT			

Change management

Version	Date	Author	Comments
1.0	13.01.2014	Sergio Filli	Initial public version

Index of open issues

Nr.	Description
1	Verification of consistency (business / technical parts)
2	Verification of consistency (main concept / add. resources)
3	Table of Rights per roles and per module
4	Definition of Report / list views
5	Definition of Data export feature