Security, KYC and Compliance

Date: **09 October 2020**

Document Revision: **1.10**

Initiation Date: **17 September 2014**

Document Revision History

Version	Date	Author	Notes
1.0	17/9/2014	Arif Saleem	Initial version
1.5	20/7/2017	Arif Saleem	Updated – 2FA, Weighted Compliance, others
1.8	31/05/2019	Arif Saleem	Updated
1.9	23/03/2020	Arif Saleem	Updated
1.10	09/10/2020	Saiful Alom	Minor updates to Remitter and Beneficiary Dynamic Risk Scoring

CONTENTS

Introduction

As a product catering to the fintech industry, the RemitONE MTS provides a range of security mechanisms and features. Additionally, for the remittance industry specifically, there are an array of KYC and compliance features that support the requirements of regulatory bodies and protect Money Service Businesses from fraudulent activity. This document outlines the salient aspects of each of these areas to give the operator a good grounding in the relevant features provided by the system.

System Level Security

The RemitONE MTS is written using industry standard development practices, such as an MVC architecture, Data Access Objects and code re-use that contribute to good quality and high security. The entire system is operated over https using high-grade SSL encryption to ensure transit data is kept safe. Even data transferred between the web application and the database server is encrypted using SSL. The web servers are fronted by a hardware Firewall and each server itself also runs a software Firewall which restricts access to only the ports required for the services provided by that server. This helps to minimise the attack vector for any malicious activity.

As the application is a web-based system, where data input can come from the Internet at large, we make use of an Intrusion Detection System (IDS) that actively scans every request made to the system and attempts to detect attacks such as SQL Injection and Cross Site Scripting. This provides a first line of defence against malicious activity. Subsequently, data written to the database is 'escaped' to prevent SQL Injection, which is a second line of defence.

All passwords are encrypted using public-private key encryption before being sent over the Internet from web browser to server, and this is done both on login screens as well as screens where user details are edited.

In order to prevent CSRF attacks (Cross-Site Request Forgery) we embed a dynamic token into every screen, which is then checked on the subsequent screen before any changes are applied. This ensures users are protected from email phishing attacks where crafted URLs are used to trick users into performing unintended actions on the system.

Server side re-calculation of transaction data, before transactions are created, ensures data protection and prevents data manipulation. Checks are performed when a transaction is created to

detect possible duplication. Limited editing of transaction details is permitted so only certain details can be altered after entry. A transaction must be marked 'deleted', and a new one created, if major details need changing. Data in the database is never actually deleted – only its status can be marked as ‘deleted’.

Audit Trail

A non-editable audit trail of major user actions is maintained within the system, that can be viewed by administrators. Actions are classified into categories and filters are provided to allow searching for specific audit actions. Some sensitive read-only actions are also logged in the audit trail, such as viewing a transaction's payout details.

When an existing entity is updated, then we also record the changes made – what the original values were and what the new values are that have replaced the original ones. This provides a very powerful mechanism for ensuring accountability is enforced.

Relevant audit entries for each transaction are also displayed on the Transaction Details screen for quick reference.

User Security

Users on the system are of different types, and functionality is restricted based on these types. Within each broad user category, there are additional sub-categories of users to provide finer grained control over user abilities. Some user types can also have individual features enabled or disabled. This ensures that user access is role based, thus preventing unauthorised actions being taken on the system.

Access Restrictions

Access to the system can be restricted by IP address on each user's profile, and multiple IP addresses can be specified per profile. This can be used to limit user access only from Office IPs, but it does require the use of static IP addresses.
Alternatively, MAC address checking can be used to restrict access from a single PC. This can be set per user, and uses a Java Applet that runs in the web browser, thus allowing cross-platform usage. (NOTE: With the deprecation of Java Applets by major browser vendors this method may not function properly).
A third method that uses hardware IDs generated on the user's PC can also be used, which is more secure than MAC address checking, but this is Windows specific.
Superior to these methods is the sophisticated Two Factor Authentication that we provide, which will be covered later in this document.

Each user profile can have start and end access times set, only allowing user's to login within those times. This again can be used to ensure that users only access the system during normal working hours. Weekend access can also be disabled, with weekend days being specified on a per-country basis.
A more fine-grained time-based access profile can also be created per-user. This allows access settings per-hour throughout the week.

Every attempt at user login or logout is recorded in a non-editable Access Log, that includes details such as the access IP address, time and result of the attempt. This ensures that Administrators can determine accurately when particular users accessed the system.

Account Locking
If an incorrect password is entered multiple times, the account is automatically locked for a 30 minute period. After the timeout period, the user can login normally with the correct password. Alternatively, the Administrator can unlock the account manually. This account locking also applies to users of the Web Service API.

If a user does not login to the system at all for a long period of time, the system can be configured to automatically mark the account as 'dormant' and then login is denied until the Administrator re-enables the account.

By default, a single user can only login once – two simultaneous logins by the same user from two different web browsers or PCs is detected and blocked.

Teller Security Features
Transactions above certain limits can be held for additional checks. This ensures high value transactions are properly accounted for. Payout transactions by tellers, particularly cash collection transactions, can be controlled through locking mechanisms and payout limits. These help to avoid fraud by internal staff.

Credit Checks
Source agent credit accounts help prevent system abuse as agents can’t create more transactions than they are authorised to. Sophisticated reporting of agent debt age, and cumulative credit and debit, over a period also help to keep track of monies owed. Delivery organisations also have credit accounts where all transactions are logged, ensuring fund transfer totals are automatically calculated and tracked by the system.

Mobile App security

The Android and iOS applications provided by RemitONE uses high grade encryption with public/private key pairs to ensure that all sensitive data is kept safe. The app also uses a PIN number that must be entered whenever the app is brought into focus from the background.

Password Security

Password security is extremely important, and if users do not use good passwords then all the aforementioned measures can be pointless. To this end the system enforces a minimum password length and complexity based on presence of small case, upper case, numbers and special characters. These rules can be configured by the administrator, though the default settings are generally of good quality.

Password Expiry and Reuse

Additionally, passwords can be set to expire after a set number of days, requiring the user to reset their password before they are able to continue. A history of previous passwords is also maintained in encrypted form, and users can be prevented from using the last few passwords in order to prevent simple alternation between passwords.

Passwords are never stored in plain text within the system, rather they are stored as a Blowfish encrypted salted hashes (Bcrypt), which is almost impossible to decrypt through brute force.

All passwords are encrypted using public-private key encryption before being sent over the Internet from web browser to server, and this is done both on login screens as well as screens where user details are edited.

Authentication Mechanisms

The default system uses it's own username and password database to authenticate users. However, it is also possible to use external authentication sources such as LDAP/Active Directory, thus allowing larger organisations to centrally manage their user credentials.

Two factor authentication

This can be implemented via a number of different methods:

1. **SMS** : An SMS message is sent to the user when they attempt to login, and the code from this

message must then be provided to complete the login process. This is simple to use, but there will be a cost for the SMS messages sent.
2. **Google Authenticator** : The Google Authenticator app needs to be installed on the user's smartphone, and this then generates a code that the user must provide at login. This is a free service from Google, but the user must have a smartphone.
3. **Email**: An email can be sent to the user's registered email address with the code that must then be used to complete the login process.
4. **Entrust Hardware fobs**: The hardware fob generates a one time password (OTP) that needs to be used to complete the login process. However this requires the deployment of an Entrust Authentication server and the issue of hardware fobs to all users.

The specific 2FA method can also configured individually on each user's profile.

KYC

Regulation in the remittance industry is very strong, and for good reason. Part of this is strong KYC rules and procedures. The RemitONE MTS provides an array of features to enforce and encourage good KYC practices.

The system forces users to capture details of remitter and beneficiary names, addresses, postcodes, telephone and mobile details, and also multiple ID documents. These details can be configured as required or optional on a per-country basis, as regulation on these details is different in different countries. Alternative address details can also be captured for remitters, allowing for travelers to provide both permanent and temporary addresses.

Up to four ID Document scans can be uploaded onto the system, and ID Document creation and expiry dates can be entered. Expiry date checking is then performed at transaction creation time, and tellers will be prompted to update ID details before continuing.

Automated ID Verification

It is possible to perform real-time online verification of KYC details using third-party data verifiers, such as GB Group, Experian or Trace Smart. This automated ID verification occurs at remitter registration on the Online Remittance Manager (ORM) or on creation of a transaction on the Agent Remittance Manager (ARM). This feature requires the MTO to obtain an account with the third-party data verifier, and charges will be levied by them per lookup.

Some of these providers can also verify the uploaded scan images of ID documents, thus providing an even greater level of verification. This becomes particularly important in the scenario of Online Remitters, either via the ORM module or the Mobile App.

Also, remitter address validation can be performed through Loqate (formerly called PCA Predict or PostCodeAnywhere) in order to ensure that address details provided are accurate and valid. Again, this requires the MTO to open an account with Loqate/GB Group and they will levy charges per lookup.

Individual vs Corporate Remitters

Corporate remitters need to be treated differently to individuals, and the system allows additional KYC data for corporates. Company details can be captured, and representatives of the company can be created as separate entries on the system. At the point of creating a transaction, the corporate entity can have a representative assigned to the transaction, so that the person actually performing the transaction can be correctly recorded as well.
Compliance rules can also be created separately for Corporates versus Individuals, as the regulatory requirements for each are often different.

Compliance Checks

The RemitONE MTS prides itself on a Compliance Engine that provides broad and sophisticated features for implementing compliance regulations and detecting fraudulent activity. There are a number of aspects to this, including volume and velocity checks, phonetic name matching, and additional pluggable compliance rules.

Volume and Velocity Checks

A comprehensive GUI compliance rules editor allows compliance rules to be dynamically created and controlled to perform complex volume and velocity checks on transactions. Velocity and volume checks when a transaction is created detect and prevent remittance structuring, also called 'linked transactions'. They can be performed against both remitters and beneficiaries, per transfer corridor. This ensures multiple transactions are not used to circumvent single transaction limit and frequency over a certain period. Time-based volume limits can be set against remitters to ensure they can’t transfer more than a certain amount during a fixed period.

Additionally, rules can be set to have ‘weights’ and then only when multiple rules trigger together, such that the total weight crosses a limit, will the transaction then be deemed a ‘failure’. This allows for an extremely powerful Compliance Rules scheme.

An additional set of Compliance Points can be configured on a separate screen, and again these points needs to cross a threshold before the transaction is flagged as suspicious. This allows fuzzy monitoring of transactions to gauge the level of risk.

Any transaction that fails these checks can be blocked entirely, marked for further examination, or forced to require additional remitter ID documents. The administrator can also force large-volume transactions to be further scrutinised before they are submitted for processing.

Blocklist name matching

The system includes a sophisticated blocklist name checker (BCM) that uses our state-of-the-art *NameMatch*™ technology to perform phonetic name matching, to determine if remitters or beneficiaries are high risk, and therefore require more stringent checks. The BCM automatically pulls data from the following sanctions lists:

OFAC
HM Treasury
EU Sanctions
UN Sanctions
Australian DFAT
Dutch Sanctions
Canadian DFATD
Monetary Authority of Singapore
French GELS list
For PEP, we retrieve data from EveryPolitician.org and the World Presidents Database.

A custom list can also be loaded into the system by your system administrator.
The system will generate a relevance score when matching names against these lists. The system can be configured to block transactions where a match is made, or ensure the transaction requires additional checks.
It is also possible to use external name screening services such as GB Group, particularly for PEP screening.

How the Relevance Score is calculated

The Relevance is used to determine whether the transaction is actually held or not. The default setting is that a Relevance of 8.0 is needed in order to hold the transaction for compliance checks.

The Relevance is the %age of name parts in the PROVIDED name that match name parts in the BLACKLIST name, converted to a score out of 10. However, for a match a minimum of two names must match. Also, the overall score will be reduced if the number of names provided is less than the number of names in the match.

The order of the name parts provided does not restrict the matches made. Also, each name part is checked both with its actual spelling and also with the phonetic version of the name. This means that different spellings of the same name will still match and produce results.

Consider the following example cases :

1. Provided name: David William Donald Cameron, Blocklist Name : David William Donald Cameron
This will be give a Relevance of 10 = 100%, since all four provided names are present in the list name.

2. Provided name: William David Cameron, Blocklist Name : David William Donald Cameron
This will be give a Relevance of 8.8 = 88%, since three provided names ("William", "David" and "Cameron") are present in the list name, but the list name has four names in it.

3. Provided name: David James William Cameron, Blocklist Name : David William Donald Cameron
This will be give a Relevance of 7.5 = 75%, since only three out of four provided names ("David", “William” and "Cameron") are present in the list name.

4. Provided name: Cameron David James, Blocklist Name : David William Donald Cameron
This will be give a Relevance of 5.9 = 59%, since only two out of three provided names ("David" and "Cameron") are present in the list name, and the list name has four names.

In addition to the actual name, the scoring engine will also filter matches where the Date of Birth matches the list date of birth, provided that data is available in the list.
When the date of birth is present in the blocklist data, and a date of birth is provided in the lookup call, then the year component (not the month and day) must match. If the year does not match then the blocklist match will be removed from the results.

Remitter and Beneficiary Duplication Detection

A major compliance issue is the detection and prevention of structuring. To this end the system performs duplication detection. These checks are based on a scoring system that can be configured, based on the fields provided.

Remitter Duplication Prevention
In the case of remitters, the duplication detection will prevent the creation of a duplicate. Instead, the teller will be informed of the remitter ID that they should use.

Beneficiary Linking and Compliance
In the case of beneficiaries, a sophisticated mechanism of linking is employed to ensure that compliance checks can then be performed across linked beneficiaries. Creation of the 'duplicate' beneficiary is not blocked, as this could result in breach of privacy and/or data protection act violations.

Compliance checks can be set on each beneficiary so that each beneficiary can only receive up to a certain amount of money or a certain number of transactions within a set period of time. To prevent users from bypassing these compliance checks by creating different beneficiary accounts for the same beneficiary, the system needs to either prevent the creation of duplicate beneficiaries or to detect and keep a track of these duplicates.

If the remitter is prevented from creating a duplicate and thereby forced to use the existing beneficiary account, it will mean they will be allowed to reuse the same values set for that beneficiary when the beneficiary was created, potentially by another remitter. Especially in the case of the ORM, this would be a breach of privacy of the beneficiary details.

It is for these reasons that we have chosen to use beneficiary duplication detection and linking. This means when the beneficiary is either created or updated, we perform duplicate detection on that beneficiary to see if other beneficiaries in the system are duplicates of that beneficiary. We do this duplicate detection based upon a configurable criteria of the beneficiary details with a threshold so that if a certain number of details match, the beneficiary will be considered a duplicate (more detail in the technical section below).

Since the system has this way of detecting duplicates, it will then perform this check every time a beneficiary is either created or updated and keep a record of the beneficiaries which are considered duplicates. Then when the compliance checks are performed, for compliance checks

dependent on the beneficiary, the compliance engine will consider the total values of all beneficiary duplicates of the beneficiary being checked (as they are considered the same person).

The admin will also have the option to override system matched duplicates in order to add their own duplicate link between two beneficiaries or to remove a system created duplicate link.

Remitter and Beneficiary Dynamic Risk Scoring

A risk score between 0 and 100 is generated for each remitter and beneficiary on creation, and rules can be applied to alter this risk score based on factors such as nationality, country of registration, name screen score and member type. The activities of the remitter or beneficiary can then be used to alter this score, increasing it for risky activities and reducing it for safe activities.

Custom Risk Score Rules can also be created to apply risk rules on transactions. When triggered, they too will add to the risk score rules. A risk core can also be added to compliance rules, and when triggered, points can be added to the risk score and the transaction can be held for compliance checks.

Conversely, if a ‘clean’ transaction is created then points can be deducted from the risk score. New compliance rules can then be created to hold all transactions where the remitter or beneficiary risk score is above a threshold, say 80 points. This allows for a very flexible method of compliance screening that rewards ‘safe’ customers with fewer checks, while adds greater scrutiny to those who perform ‘risky’ transactions.

The risk score is shown clearly in a colour coded fashion when creating a transaction, so Agents and Tellers have a clear idea of the transaction they are dealing with. Additionally a history the changes to the risk score log can be viewed to understand how a particular customer’s risk score has changed over time.

A Risk Report can be run to show the custom Risk Score Rules, that were triggered during a particular period, along with other criteria.

Bureau de Change Compliance Checks

Separate velocity and volume compliance rules can be configured for FX/Bureau de Change

transactions. These rules can trigger FX transactions to be blocked or held for approval, just like remittance transactions.

Compliance Transactions Checks

A third category of transactions is the Compliance Transaction. These are transactions imported into the system purely for monitoring purposes and not for processing or paying out. A web service is provided to push these transactions into the system, and custom Velocity and Volume compliance checks will apply to these transactions.

Pluggable Compliance Modules

New modules can be plugged easily into the system so other custom checks can be added. The results must be examined and accepted by the source agent before a transaction can be created.

For example, custom checks based on additional remitter data, such as annual income or expected annual remittance, have been implemented in this way. Also, integration with third-party data verifiers such as GB Group, Experian, World Check etc can be implemented as a pluggable module.