PSQR SOFTWARE

Saga Compliance Suite for Chestny ZNAK (CRPT)

Comply with the Russian Traceability Regulation and seamlessly connect with Chestny ZNAK (CRPT)

INTRODUCTION

Bigger demand for sound traceability practices

> Across the globe there is a bigger demand from governments for sound traceability practices.

The European Tobacco Products Directive (TPD), Medical Device Regulations (MDR), Framework Convention for Tobacco Control (FCTC) and the Russian traceability regulation have all caused businesses to reshape their operations and digitise their supply chains.

Itemised traceability a reality for Russia

Resolution No. 792-r published by the Russian Government on 28 April 2018 has made itemised traceability mandatory across industries, including but not limited to tobacco, apparel, pharmaceuticals, dairy, food and beverages.

This regulation is not only applicable to companies within Russia, but also to those who trade or export to Russia.

According to the Russian Ministry of Industry and Trade, over 6 million counterfeit products have been identified in the Russian market since early 2018. This is having a negative effect on the trust that consumers have in the products they acquire, which in turn leads to reputational damage and financial losses.

Serialisation and supply chain data collection

> Serialisation and the application of digital markings enable manufacturers, distributors and all parties in a supply chain to gather information about products.

Thus, ensuring that they can track and tell the true story of the origin, journey, whereabouts, and consumption of products and resources across the respective supply chains.

In this regard, the Russian Centre for Research in Perspective Technologies created Chestny ZNAK, a digital track and trace system, which is geared to handle and manage global traceability projects. The main objective of the system is to increase the level of security for Russia's fight against counterfeit and low-quality analogues. It also supports the implementation of the mandatory product markings on products across Russia.

Chestny ZNAK and CRPT

> With Chestny ZNAK, special digital codes are used to guarantee the authenticity and quality of the goods. Manufacturers or importers are required to apply digital markings on all products, so that the necessary information about the products can be gathered.

The code can include the manufacturer's name, date of production, expiration dates and much more.

When these codes are scanned or detected at different points in the supply chain, like transport, merchandising or at point of sale, information gets automatically added to the system. By using a mobile application, consumers can scan the digital markings and verify the product authenticity and provenance.

The vast amounts of data collected is stored in the Russian State's information system called CRPT, creating a national catalogue of goods.

It is required that Russian manufacturers and distributors work with Chestny ZNAK and CRPT for the serialisation guidelines, to obtain codes, as well as to register on the monitoring system.

PSQR

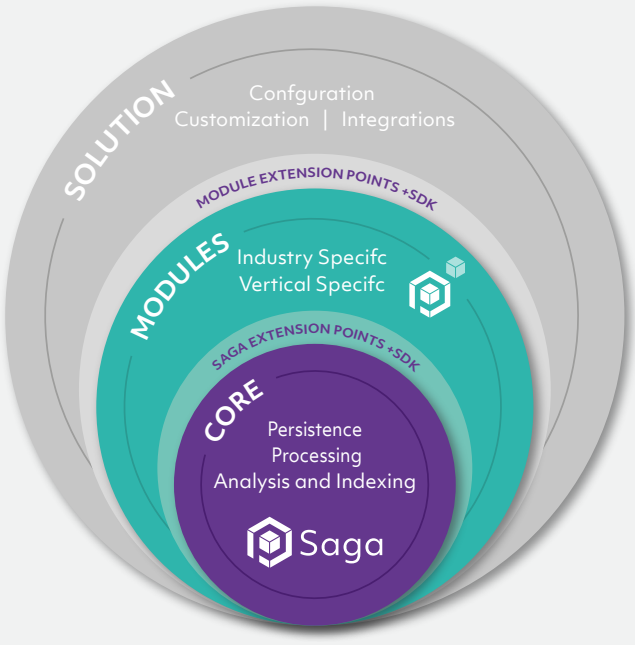
THE SAGA COMPLIANCE SUITE - CHESTNY ZNAK (CRPT)

This document outlines the technical aspects and architecture of our Saga Compliance Suite - Chestny ZNAK (CRPT).

PSQR has developed a software stack that manufacturers and distributors can use and easily integrate into their current systems, to ensure compliance with the Russian traceability regulations.

The Saga Compliance Suite - Chestny ZNAK (CRPT) consists of our Saga Compliance Suite and a specialised sub-module that has been specifically crafted to ensure optimal data exchange with Chestny ZNAK and CRPT.

INDEX



Saga's highly scalable and modular architecture allows for unique adaptations and solutions for industry and customer needs.

Saga is used as the core of all of our software solutions. It is then complemented by a set of modules, extension points and customised configurations.

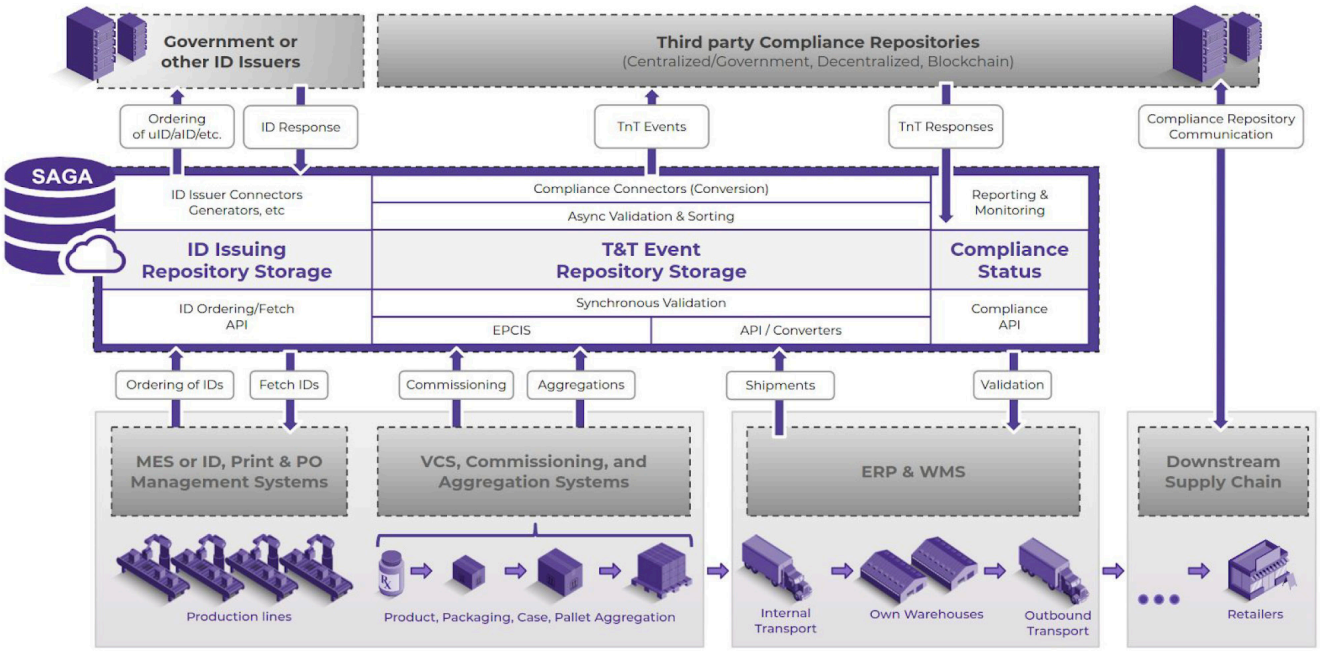
This modular set allows PSQR and our partners to create unlimited solution applications for most industries across the globe.

PSQR

Saga Compliance Suite

The Saga Compliance Suite is based on the GS1 standard EPCIS. It has been implemented in a number of industry solutions globally, providing all the functionalities needed for a complete compliance solution where codes are issued and used for collecting and sharing track and trace data .

> In essence, the Saga Compliance Suite enables both the manufacturer and importer to generate or fetch IDs (or codes) from authorities and share or report the track and trace information as required.



Saga Core provides the basic track and trace functionalities including a highly scalable and flexible EPCIS based event repository. The ID Module brings standard APIs and ID processing and storage to Saga. The Compliance Module brings asynchronous validation and processing of events to external repositories, including a repository for storing the compliance status of the events.

> An instance of the Saga Compliance Suite is composed of the following components:

- Saga Core
- ID Module
- Relevant ID Connector Sub-modules
- Compliance Module
- Relevant Compliance Connector Sub-modules
- Other relevant Saga Modules
- Customer/Solution specific Configuration

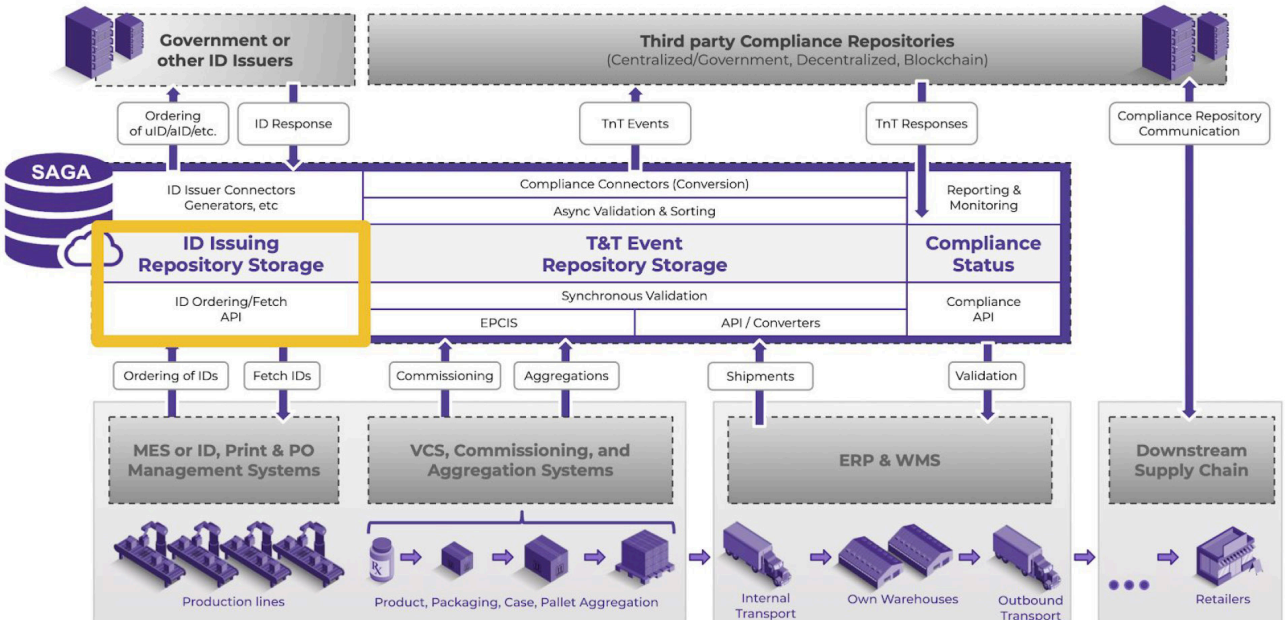
Saga

ID Module

The ID module provides a framework for connecting to third party ID Issuers, store IDs, and make them available via generic APIs. The module also exposes extension points through which ID Connectors (Sub-Modules) can be registered.

> This module and connectors are responsible for:

- Sourcing, storing and tracking IDs from multiple sources
- Validation of ID ordering to ensure consistency
- Providing the IDs via a generic API



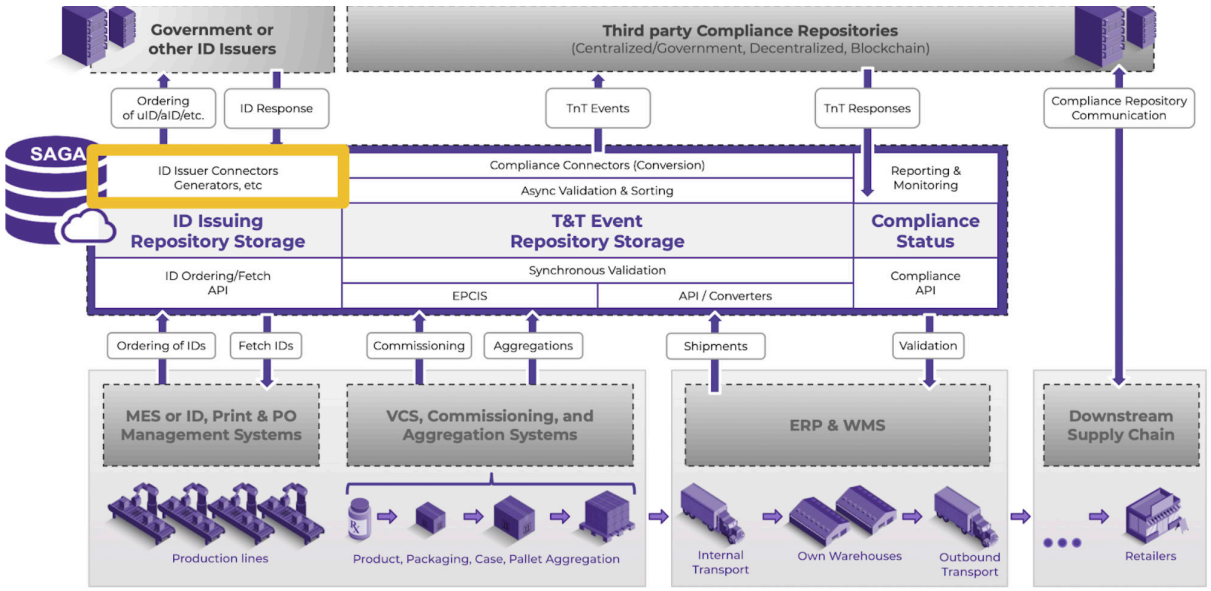
Production Order Management Systems or Manufacturing Execution Systems typically running on premise will use the APIs to order and download IDs. These local systems will then apply the IDs on products, typically as 2D barcodes, but in some cases also in human readable format - or a combination hereof.

ID Connectors (Sub-Modules)

> The connectors are specific to one or a small group of ID Issuers. The ID Issuers are typically run by a government entity of some form, and depending on their compliance scheme the IDs can either be:

- Generated by the manufacturer themselves
- Ordered and downloaded from the ID Issuer
- Generated and signed/registered into the ID Issuer

Saga



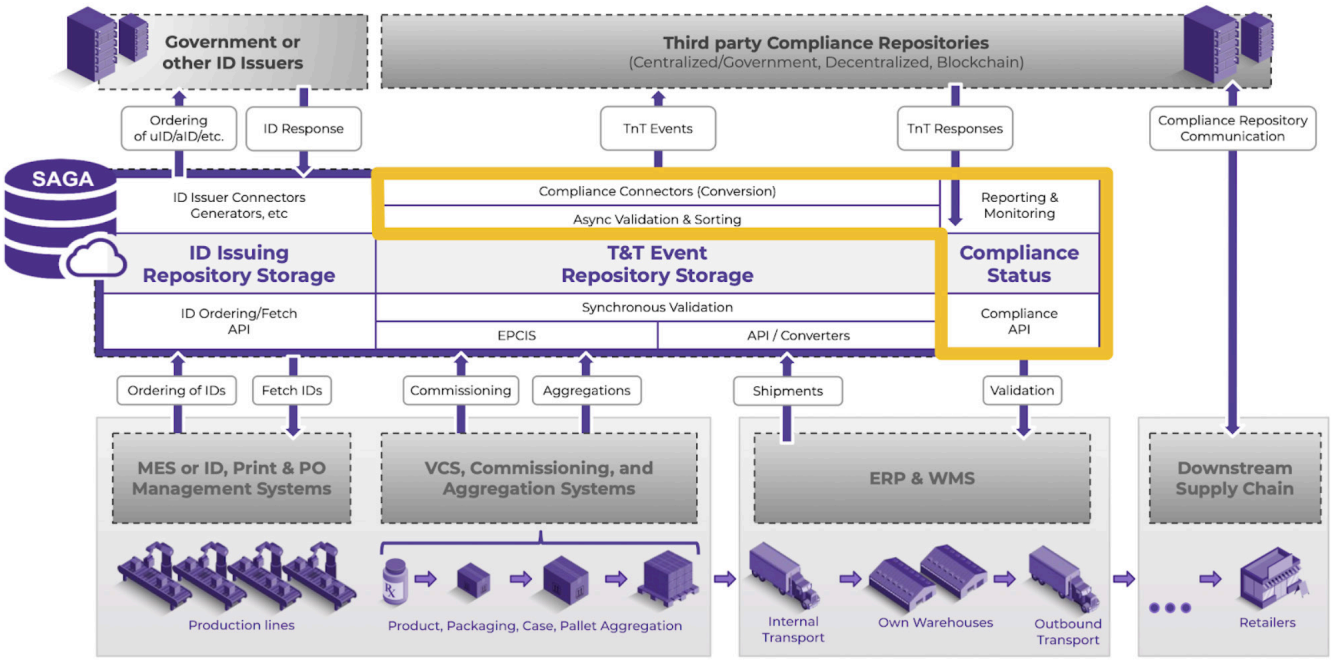
Which IDs must be ordered/downloaded/signed and which ones can be generated often depend on the level in the package hierarchy.

Compliance Module

The generic compliance module contains all the functionalities that are common to the compliance validation process with any third-party compliance repository. The module is extensible and multiple Compliance Connectors (Sub-Modules) can be registered.

> The overall responsibilities of the module are:

- Processing events through registered connectors
- Ensuring correct event sequencing
- Validating events against business rules
- Converting the events to a compliance repository format
- Sending the events to one or multiple compliance repositories
- Fetching and storing the event compliance status
- Handling validation and compliance failures
- Reprocessing events
- Reverting events



> When processing events, the generic compliance module forwards events to the relevant compliance connectors to obtain a successful compliance status.

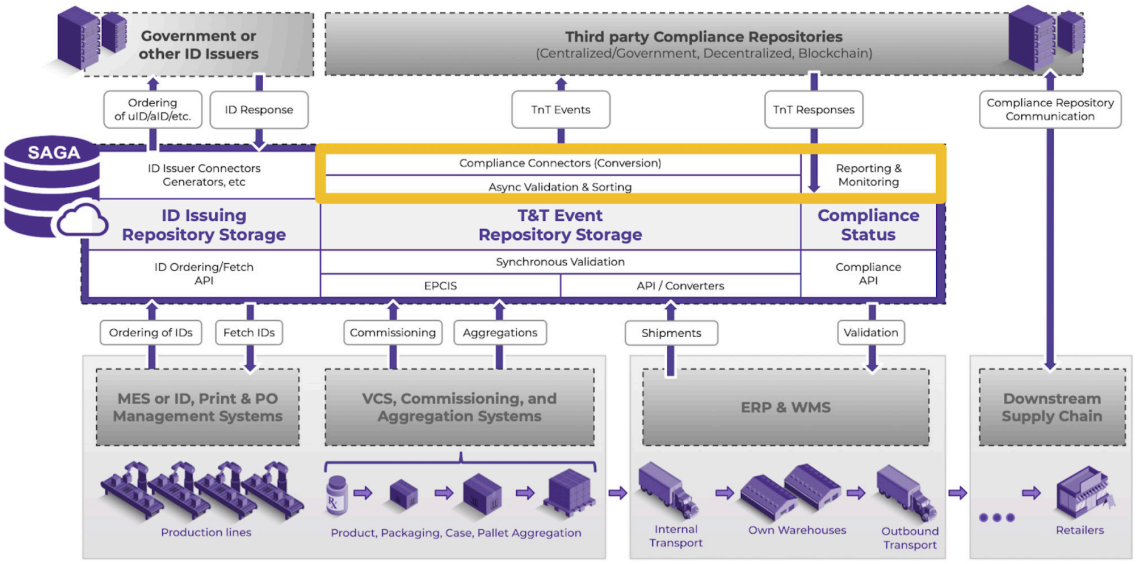
After the validation, conversion and forwarding of the events to the relevant compliance repositories has been done by the connector (sub-module), the generic compliance module stores the compliance status received from the compliance repository into its compliance status data store.

If the sequence check, business rules validation, or compliance check of an event fails, the event is stored by the generic compliance module. Depending on the failure reason, the event may be reprocessed automatically until a predefined maximum number of attempts. The failed events that cannot be reprocessed automatically or for which the maximum number of reprocessing attempts has been reached are stored by the compliance module and can be fixed and reprocessed manually.

In the case of out-of-sequence events, the generic compliance module will postpone processing of events until the events they depend on have been successfully processed. The dependent events will retry based on a time schedule, but will also be reprocessed immediately after successful processing of the blocking event using the wake-up feature of the compliance modules.

Compliance Connectors (Sub-Modules)

Each compliance repository has its own rules and format for events. Therefore, the compliance module, being generic, requires connectors (sub-modules), built specifically for each third-party compliance repository in scope. These sub-modules contain the logic to communicate with that repository and to validate events according to its rules.



> Connector sub-modules make use of extension points in Saga and in the generic compliance module. Their responsibilities include:

- Implementing events sequencing rules
- Validating events against business rules
- Converting events to the relevant compliance repository format
- Sending them to one or multiple compliance repositories
- Processing the response from the compliance repository
- Reverting (or recalling) events

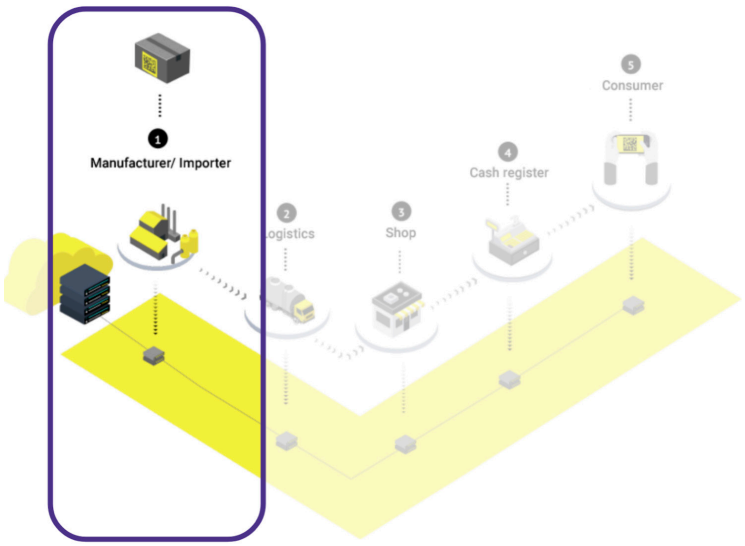
A connector sub-module is a layer built on top of the generic compliance module that contains all the configurations that are specific for a compliance repository.

Those configurations include sequencing rules, business rules, master data mapping, and conversion rules. After being processed by the generic compliance module, events are validated by the connector sub-module against the compliance repository sequencing and business rules. When the events are validated, they are converted to the repository event format and forwarded to the repository. Depending on the rules of the compliance repository, events can still be reverted (recalled) after being forward to the repository.

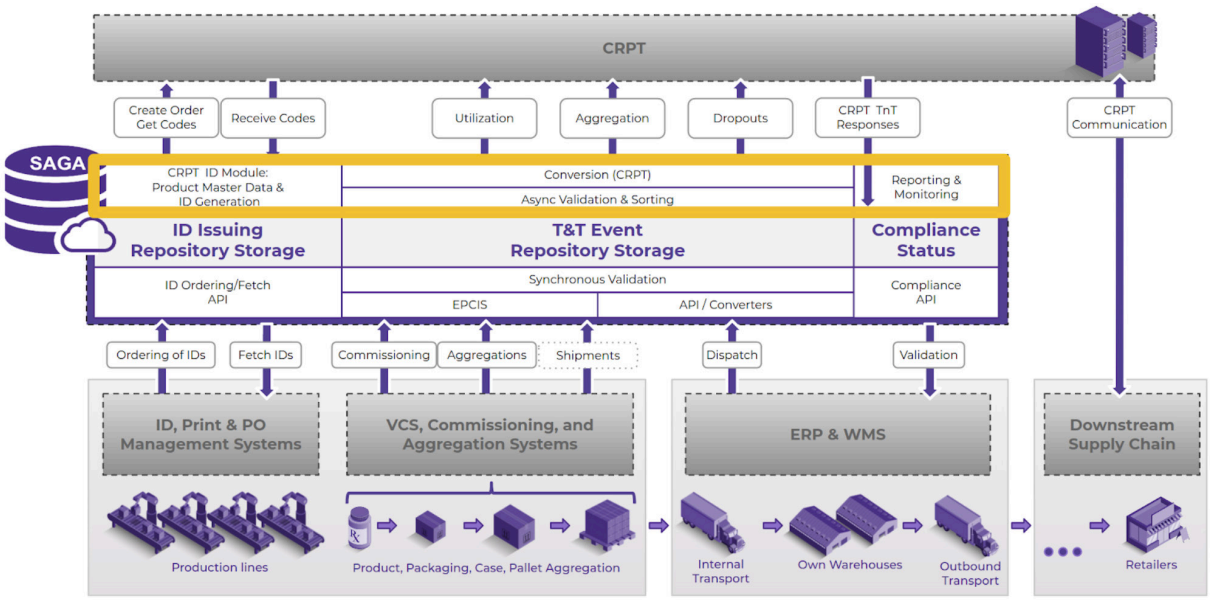
Connector sub-modules for different third-party compliance repositories share most of their code, differing only on the configurations needed for each repository and, possibly, small functionalities that may be required by each of them.

Chestny ZNAK (CRPT) Sub-Module

> This Saga sub-module has been specifically crafted to ensure optimal data exchange with Chestny ZNAK (CRPT). Hereby assisting in compliance with the Russian traceability regulation. The Saga Chestny ZNAK (CRPT) Sub-Module focuses on goods to be imported into Russia.



The CRPT Module is a sub-module for both the ID Module and the Compliance Module and hence contains connectors for both. The module allows for ordering IDs (codes) which will then be made available to on-premise production systems for printing. Once printed these codes are reported back to Saga as commissioning and/or aggregation events. Based on these events the CRPT connector creates the relevant messages and sends them to CRPT for activating the codes.



The Chestny ZNAK track and trace scheme covers a number of different product types which must be serialized and reported on.

The requirements for how the codes are constructed, what data elements they must contain, their longevity, etc. may vary. All of this can be taken care of by utilising the CRPT Module in Saga.

> The ID Connector of the CRPT Module will allow generic ID ordering requests to be transformed into CRPT specific requests and will take care of the successful download of these. The ID Connector thereby:

- Provides the generic ID ordering API of the ID Module to production systems
- Ensure relevant MasterData is present when ordering IDs (Codes)
- Order CRPT generated codes or generate codes for CRPT signing
- Securethe code (crypto part)
- Handle both product and aggregation level codes
- Poll orders to fetch IDs (codes) as early as possible
- Allow manufacturers or distributors to inspect downloaded codes

> All events related to the items labelled with the UIDs are tracked and traced and forwarded to CRPT through the Compliance Module and the CRPT connector sub-module, which provide the following functionalities:

- Processing of events
- Checking events sequencing
- Validating events against business rules
- Converting events to CRPT format
- Forward events to CRPT
- Reprocessing failed events
- Reverting events
- Getting the event compliance status from CRPT and storing it in Saga.

Saga

PSQR - We are Track and Trace Software Experts

PSQR is a Danish software development company that specializes in highly scalable software for storing, processing and analysing vast amounts of supply chain data. The company partners with track and trace software integrators, solutions providers, consultancies and industry bodies to bring best of breed IT Solutions to the world of Traceability. Hereby empowering manufacturers, corporations and governments across the globe with digital track and trace capabilities and the ability to tell the true story of the origin, journey, whereabouts, and consumption of products and resources across the supply chain.

Reach us at www.psqr.eu and on LinkedIn or send us an email at info@psqr.eu

PSQR

Frederiksborggade 15 | 6-7th floor | DK-1360 | Copenhagen | Denmark