TORP.

Onboarding and Origination CX platform

Product overview

Table of contents

01. **Executive** Summary

–

We are pleased to present in the below sections Tremend's Digital Onboarding and Origination platform - TORP, including details regarding the functionalities, implementation, integration and support services, based on Tremend's methodology framework.

We are confident that we are in a position to deliver a sound proposal that fulfils your expectations.

We consider TORP - the origination platform built by Tremend - as the best fit, as it exceeds the requirements of the project, it brings a set of industry-wide best practices and leverages on the existing expertise of Tremend's Subject Matter Experts. The TORP product team involved in this project has a substantial experience working with the required methods, technologies and tools, proven expertise and track record, with strong expertise in implementing complex projects, a large number of varied stakeholders and end-users, and high level of commitment, passion, and responsibility required to complete critical tasks successfully.

02. **Tremend.** Company Profile

–

2.1. Overview

Tremend Software Consulting is a top Romanian software provider, with over 14 years of experience in delivering complex software solutions that incorporate advanced technologies. Tremend has been nominated by Deloitte, Financial Times and Inc. Magazine as the fastest-growing tech company in Romania and in top 50 in Central Europe.

With a strong engineering DNA, Tremend is proud to be a reliable technical partner for some of the world's renowned organizations. Tremend has completed over 700 successful projects for 200+ customers, from Fortune500 to innovative startups in over 20 countries.

The solutions developed by 400+ experts are being used by over 60 million users and target leading companies in industries such as retail, manufacturing, finance, telecom, automotive and healthcare.

Tremend delivers professional services for over 150 clients in Europe, Asia, Australia, and North America, with some of our most notable clients including:

- **EMEA** (France, UK, Germany, Switzerland, Austria, Belgium, Denmark & others) - Santander, European Bank for Reconstruction and Development, Essentra, Ingenico, European Commission, etc
- **AMER** (US, Canada) - Intel, Netflix, Sanmina Corporation, Atlanta Airport, WindRiver, etc
- **APAC** (Asia & Pacific) - NVidia (Mellanox), Ceragon, etc
- And in **Romania** many of the top 50 companies: Orange, Carrefour, Dacia, BRD, E.ON, Auchan, Vodafone, Raiffeisen Bank, ING Bank, etc

The expertise in business solutions currently covers:

- Agile Enterprise
    - Omnichannel Customer Experience Portals
    - Enterprise Content Management
    - eCommerce & Marketplaces
    - Internet & Mobile Banking platforms

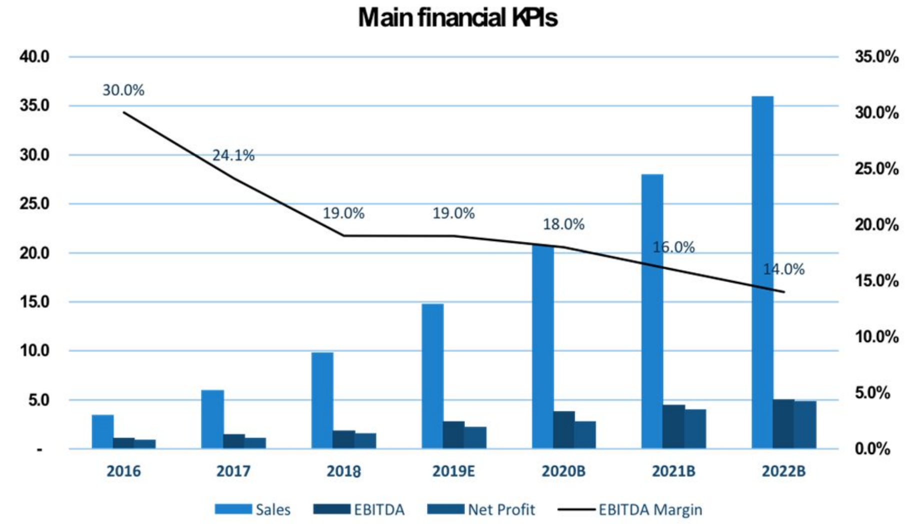
- Advanced Engineering
    - Car Infotainment systems
    - ASIC design & Firmware
    - IoT - End-to-end
- Emerging technologies
    - Machine Learning & AI
    - Biometrics
    - Blockchain
    - RPA

Tremend has three development centres in Romania, in Bucharest and Brasov, one in Vietnam, and sales offices in the US, UK, and Belgium.

2.2. Business evolution

We maintained the double-digit growth rate in 2019 and we anticipate to accelerate in 2020.
The growth is sustained by accelerated growth of FTEs to service both the up-sale on existing clients and the acquisition of the new business. We secured in this respect a 3 years contract of EUR 9m, among other commitments.

Year	Turnover EUR'mil
2016A	**3.48**
2017A	**5.93**
2018A	**9.79**
2019E	**14.85**



03. **Tremend.** References

–

3.1. TORP - project in a Telecom company

Tremend is currently integrating TORP digital onboarding and origination solution with web and mobile solutions for various clients, among which one of the major players in the Telecom industry.

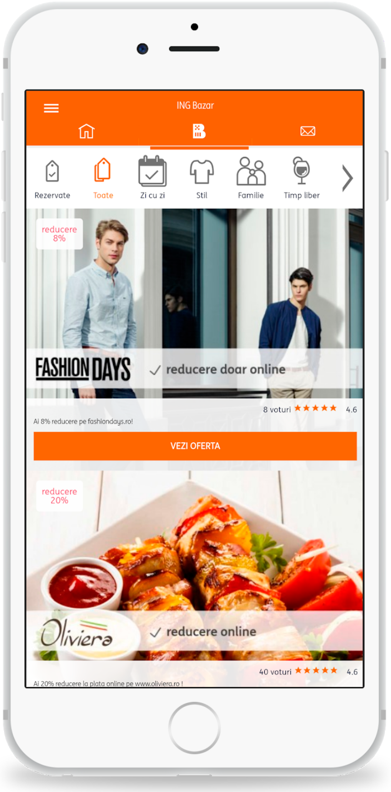
TORP has been selected as the solution of choice for electronic identification services for their prepaid services users, to comply with the most recent prepaid registration regulations. TORP framework is used for both scanned Identification Documents and Face Recognition, for both customer enrollment and originations workflows.

3.2. Mastercard Partnership

Tremend entered into a strategic global partnership with Mastercard to digitize the payments ecosystem. Enrolling cards in the mobile eWallet and implementing the Strong Customer Authentication mandate, part of the revised Payment Services Directive, are among the first projects that will benefit from Tremend Software Consulting's expertise.

The revised European Payment Services Directive (PSD2) is a key EU initiative to make online payments safer, to facilitate innovation and competition by opening banking services to FinTech and other interested companies, representing the transition of European banks to the Open Banking model. Open Banking will accelerate the transition from traditional, internalized and local financial services to digital financial services available anywhere within the European area.

3.3. ING



Ai 8% reducere pe fashiondays.ro!

Ai 20% reducere la plata online pe www.oliviera.ro !

ING is a well known global financial institution and the world's 18th largest corporation by revenue.

Tremend has a strong ongoing partnership with ING, started more than 6 years ago, covering the entire digital presence of the Bank: ING.ro Website, ING Home Bank and ING Bazar, a complex card-linked loyalty solution.

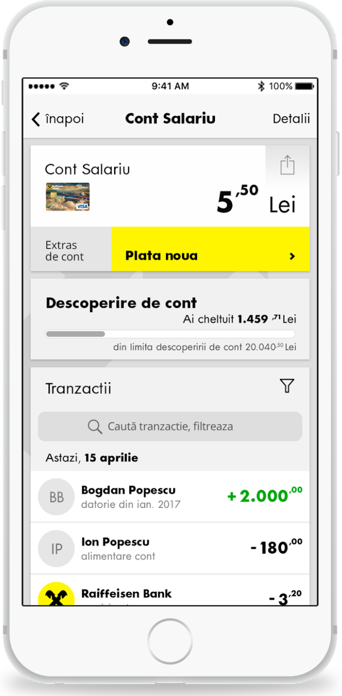
ING Bazar is a marketplace mobile app, presenting discount campaigns for ING's card users. Each campaign has its own dedicated page and users can book the discounts they are interested in, as a limited number of discounts is available in each campaign. The system delivers real-time filtering with more than a dozen criteria over hundreds of millions of transactions for millions of users.

Magento has been chosen as the best fit to replicate the shopping process that happens behind the scenes. Significant customizations of the open-source platform were required to pass security auditing and penetration testing. Since the system is real-time with zero caching, Magento's bootstrap process was dramatically improved in a concentrated effort that resulted in amazing response times.

Building Bazar solution from scratch, using a dedicated Scrum team, Tremend helped ING Bank turn its ambitious ideas into a highly scalable platform that successfully serves bank's clients.

The application has been built and maintained by Tremend specialists for over 6 years, passing through several phases of growth, from being used as an external application to being integrated into the ING's mobile banking app (the most used mobile app for a bank in Romania) and to group-level adoption in many other countries.

3.4. Raiffeisen Bank



Raiffeisen Bank is a top universal bank on the Romanian market, providing a complete range of products and services to private individuals, SMEs and large corporations via multiple distribution channels: banking outlets, ATM and EPOS networks, phone-banking and mobile-banking.

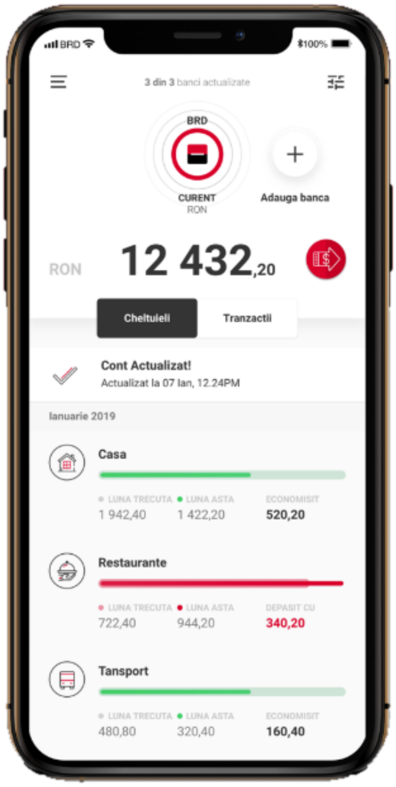
Tremend re-architectured, built and maintained a new generation of Internet and Mobile Banking Systems for Raiffeisen Bank Romania for over three years.

The solution is aimed at the over two million clients, including 100.000 small and medium enterprises, 5600 corporations and 1.9 million individuals and represents a state-of-the-art microservices architecture to facilitate efficient communication between the browser, the mobile apps and the bank's core systems.

The collaboration led to the development of an extremely flexible solution for online and mobile banking, which accelerates the Bank's response to the users' requests and allows launching new applications within days.

By developing this solution, Tremend contributed to the digital competitiveness of a major player in the financial sector, in a time of radical transformation for the industry.

3.5. BRD - Groupe Société Générale



BRD is a Top 3 Romanian Bank, part of **Société Générale Group**, sixth largest Financial Institution in Europe.

Part of the strategic partnership with MasterCard and relying on the strong expertise in cards processes flows, regulatory framework and cards systems infrastructure, Tremend participated in the implementation of the Strong Customer Authentication (SCA) mandate in BRD, the first MasterCard issuer in Romania.

SCA mandate implementation required enhancements in multiple transactional layers and channels (Mobile Banking System, Core Banking System's ESB, Cards Host System, 3rd party provider - Romcard, POS terminals) and imposed a sustained effort to complete the analysis, integration and the end2end testing phase, where Tremend's Business Analysts, Software and QA Engineers were the key players.

Using a dedicated team and offering full support and technical consultancy, Tremend helped BRD to be one of the first Romanian Financial Institution to be PSD2 SCA compliant, with the following common goals:

- Put customers in control to make informed decisions;
- Build trust and security into every payment experience;
- Expand access to data, while keeping it protected.

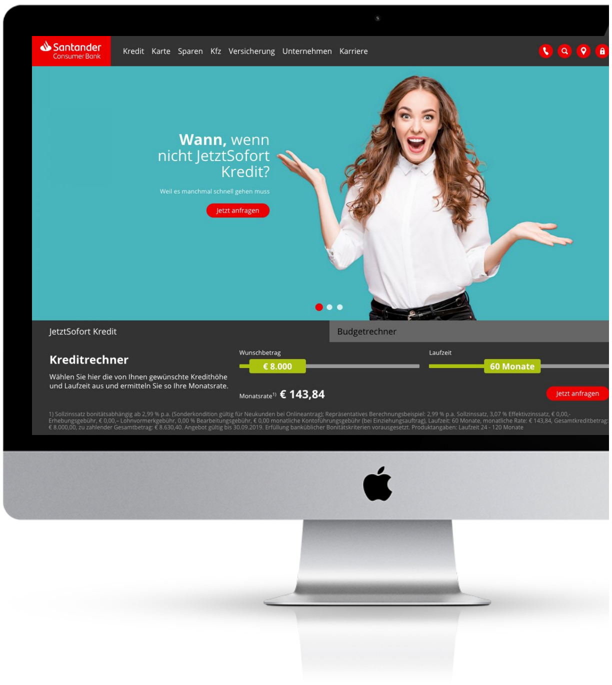
3.6. Santander Consumer Bank

Santander, one of the largest banks in the world and the biggest in Spain, needed a partner with the required experience and know-how for a technical upgrade for their solution in Austria.

Establishing a long-term partnership with Tremend, the company managed to successfully start moving from its complex monolithic solution to a solution based on microservices and continuous delivery.

Dolphin, the main legacy system using Java technologies is currently being maintained and improved by a team of 10 engineers with a parallel effort coordinated by Tremend to transform the organization to use Agile methodologies.

Having a solid platform to build upon, services like digital process platforms are continuously added to the platform.



Wann, wenn nicht JetztSofort Kredit?

Weil es manchmal schnell gehen muss

Kreditrechner

Wählen Sie hier die von Ihnen gewünschte Kredithöhe und Laufzeit aus und ermitteln Sie so Ihre Monatsrate.

Monatsrate[1)] **€ 143,84**

1) Sollzinssatz bonitätsabhängig ab 2,99 % p.a. (Sonderkondition gültig für Neukunden bei Onlineantrag); Repräsentatives Berechnungsbeispiel: 2,99 % p.a. Sollzinssatz, 3,07 % Effektivzinssatz, € 0,00,- Erhebungsgebühr, € 0,00,– Lohnvormerkgebühr, 0,00 % Bearbeitungsgebühr, € 0,00 monatliche Kontoführungsgebühr (bei Einziehungsauftrag), Laufzeit: 60 Monate, monatliche Rate: € 143,84, Gesamtkreditbetrag: € 8.000,00, zu zahlender Gesamtbetrag: € 8.630,40. Angebot gültig bis 30.09.2019. Erfüllung banküblicher Bonitätskriterien vorausgesetzt. Produktangaben: Laufzeit 24 - 120 Monate

04. **TORP.** Software solution

–

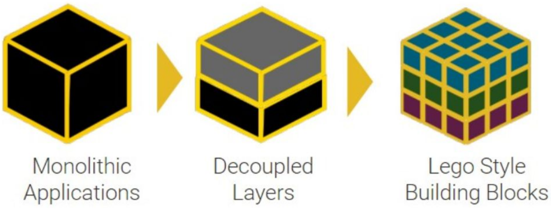
4.1. Overview

TORP is a modular platform, relying on a building block architecture, client-tailored to facilitate the adoption of flexible banking processes and product lending workflows.

The solution is easy to customize and adapt, providing high-level process automation with a focus on the business needs, supporting various channels: the Direct Sales Agents, the Branch SalesForce or a pure-online process flow, managed solely by the client.

The platform provides complete & in-depth access to all core layers: workflow management, forms builder, access management, document generation and management, data management and processes audit trails. The main goal of the framework is to facilitate the client on-boarding and lending processes, increase the number of automatic approval and disbursement, compliant with the most demanding industry-wide policies, tolerances and risk appetite.

The Building Blocks architecture is ready to use, interconnected, grouped in stand-alone functional entities, configurable with a minimum effort, relying on a state-of-the-art microservices architecture which facilitates efficient communication between the browser, mobile apps and the Bank's Core Systems.



Confidential

4.2. TORP components

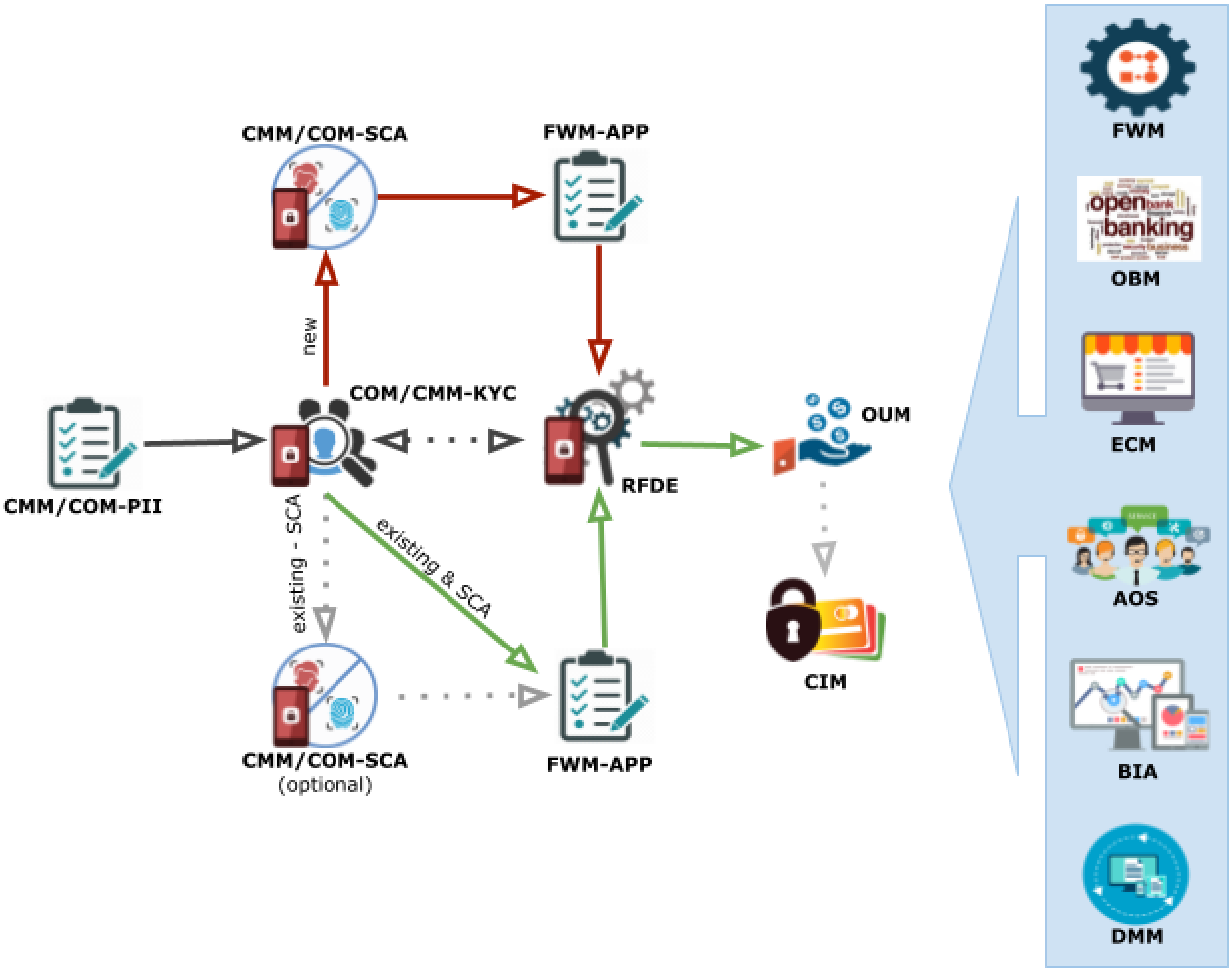
Tremend Origination Platform (TORP) relies on the following Functional Entities - a group of interconnected building blocks:

Universal Functional Entities:

- Flexible Workflow Module (**FWM**)
- Document Management Module (**DMM**)
- Assisted Online Support (**AOS**)
- Business Intelligence & Analytics (**BIA**)
- Customer Onboarding Module (**COM**)
- Customer Management Module **(CMM)**
- eCommerce Module (**ECM**)

Financial Sector Functional Entities:

- Risk & Financial Decision Engine (**RFDE**)
- Objects Upload Module (**OUM**)
- Cards Interface Module (**CIM**)
- Open Banking Module (**OBM**)



Universal Functional Entities / Building Blocks grouping:

FWM Flexible Workflow Module	**DMM** Document Management Module	**AOS** Assisted Online Support
Core (BPMN execution engine)	Core (document generation using a template)	Core (Call Me / messaging)
FWM Designer	DMM Designer	Chatbot extension
FWM Access Management	Digital Certificate issuance and Electronic Signature*	Documents exchange
	DMS integration	Voice/Video call
	Documents Upload	Real-time remote assistance
	Documents OCR integration	
	External eArchive integration*	

BIA Business Intelligence & Analytics	**COM** Customer Onboarding Module	**CMM** Customer Management Module	**ECM** eCommerce Module
Core (WEB UI, BB integration, stats, audit trail)	Core (interfaces with 3rd parties, customer data repository)	Core (customer data repository, master & detail views)	Core (back-office integration, Open Banking integration)
Native IOS and Android versions	Phone/email validation using OTP/C-R	Customer Data Update	Catalog Management
Enrollment Report	ID Card scan & OCR*	GDPR module	Content Management
Application Report	Face Recognition and selfie vs ID photo comparison*		Customer Management
	Unassisted Video Identification*		Order Management
	Assisted Video Identification*		Discount & Promotion Management
	SCA enrollment and authorization flow		Prepayment and Invoice Management*

Financial Sector Functional Entities / Building Blocks grouping:

RFDE Risk & Financial Decision Engine	OUM Objects Upload Module	CIM Cards Interface Module	OBM Open Banking Module
Core (DMN execution engine, FWM integration)	Core (CBS upload)	Core (3rd party integration: payments processor, CMS)	Core (interfaces with MasterCard Open Banking)
RFDE Designer	DMS upload	Cards issuing flow	Account Information Service*
Interface with Bank's Scoring engine	Centralized Customers Repository upload	Apple Pay integration	Payment Initiation Service*
AI Scoring*	DWH upload	Google Pay integration	
Customer screening against global watch-lists interface	Cards Management System upload	FSI's own wallet integration	
Centralized Customer Repository interface			
DWH interface			
ANAF interface			
Credit Bureau interface			
Interface with Bank's systems (Anti-Fraud, AML, ANAF, CB)			

*Note *: Building Blocks with limited usage based on the Licensed Capacity*

4.3. Technical approach

This section covers technical aspects of the proposed software solution: the solution architecture, TORP-centric, with all potential integration points, the technological stack of the software solution as well as technical breakdown and artefacts.

4.3.1. Solution architecture

The diagram below describes how TORP components interact with 3rd party providers for document signing and electronic identification, as well as the interaction with the Bank's internal systems.

The customer enrollment process starts either from the Bank's website or from the mobile app. Requests are taken over by TORP, which further integrates with the Bank's systems and TORP partners ecosystem services.

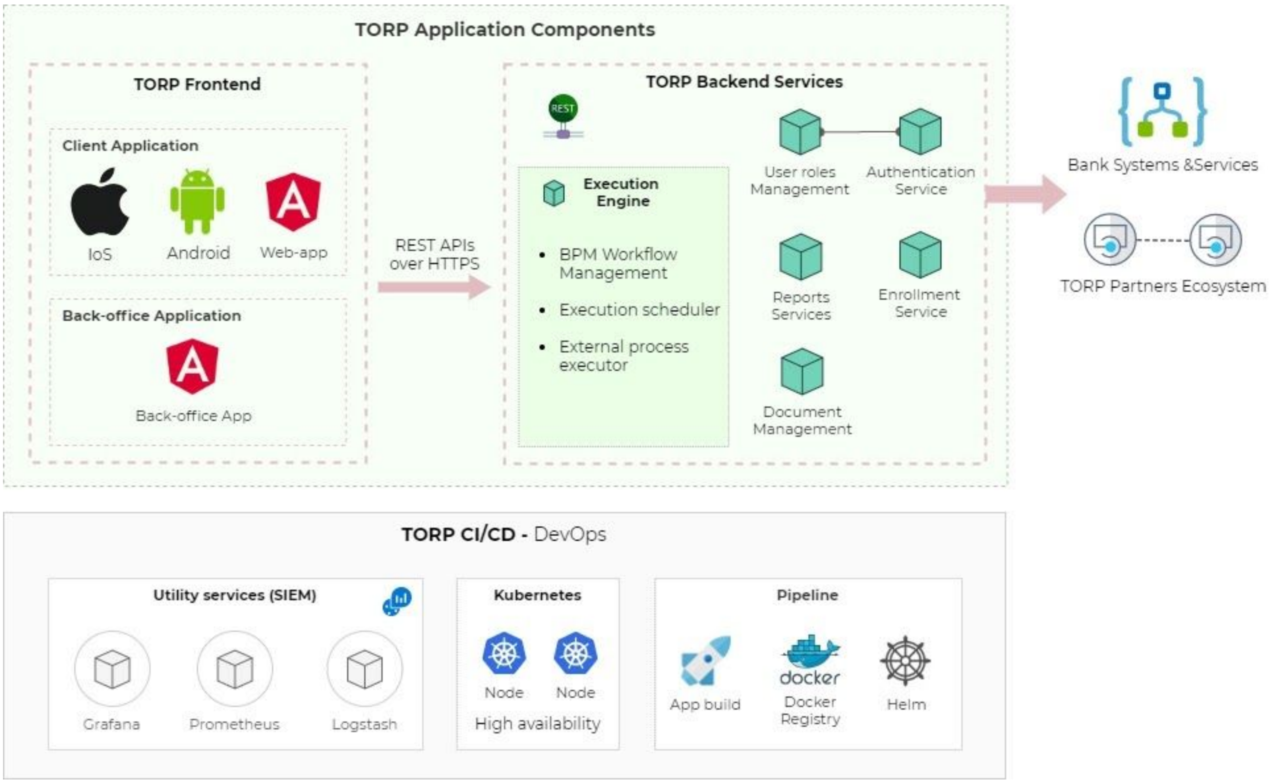


Fig.1 Solution Architecture

4.3.2. TORP Components

The following endpoints are exposed by TORP:

4.3.2.1. Back-office Application

This module is responsible for exposing the sales agent's UI capabilities (authentication, flows, document management, reports, etc). It interacts with the TORP Module in order to obtain the required information to display. Technology stack: Tremend Application Foundation, Angular, Spring Boot, Spring Data, PostgreSQL.

4.3.2.2. Core Module

This module is responsible for managing TORP's core functionalities. All the flows, the generated UI (based on the defined flows) are managed by this module. This module is also responsible for data consistency, retry mechanisms, authorization, receiving information from the other modules, especially from the TORP connectors. Each connector is called by the flow step in which it was configured (each flow's step can be linked with a connector in order to push/pull information from external systems). Technology stack: Spring Boot, Camunda BPM, PostgreSQL

4.3.2.3. KYC Module

This module is responsible for managing the Know Your Customer (KYC) process. It exposes API for JS/mobile SDKs, it interacts with de TORP Module for core functionalities like flow management and persistence.

4.3.2.4. OCR Module

This module represents a facade for the integrated OCR solutions. Its main responsibilities are related to transforming the third party OCR output in OCR input for TORP. It is built in a modular way so that the new system can be easily enrolled (eID, AriadNEXT, Microsoft Cognitive Services, etc).

4.3.2.5. Address Tokenization

This module is responsible for parsing the address retrieved from the OCR process. Initially, the tokens will be country, city/village and the rest of the address content. Later on, the module will be enhanced to support more granular tokenization (street, flat, district, etc).

4.3.2.6. Connectors

This module is responsible for managing the required integration points. In order to do that, for each integration point, a connector is implemented. The connector will transform the external system's response to TORP internal data structures. Each response is mapped with the current flow's correlation id for traceability. The information retrieved by the connector will be persisted in the current flow data structures, and eventually in the database.

4.3.2.7. Workflow Module

This module is responsible for managing the BPMN standard workflows, including the embedded forms, access management, versioning, and logging.

4.3.2.8. Document Management Module

This module is responsible for managing the document templates used throughout the workflows, for back-office WYSIWYG editor, populating the template with data collected in the workflow, the electronic signature using **certSIGN** services and document export in PDF format.

4.3.2.9. Reporting Module

From the Reporting Module, the back-office user can access the standard Customer Enrollment, as well as the custom developed reports.

4.3.3. Technology stack

4.3.3.1. TORP Frontend Applications

Below (Fig. 2) is a diagram of the technological stack used in both TORP frontend applications:

- Direct Sales Agent Application (DSA)
- Back-office
- Customer applications (WEB and mobile)

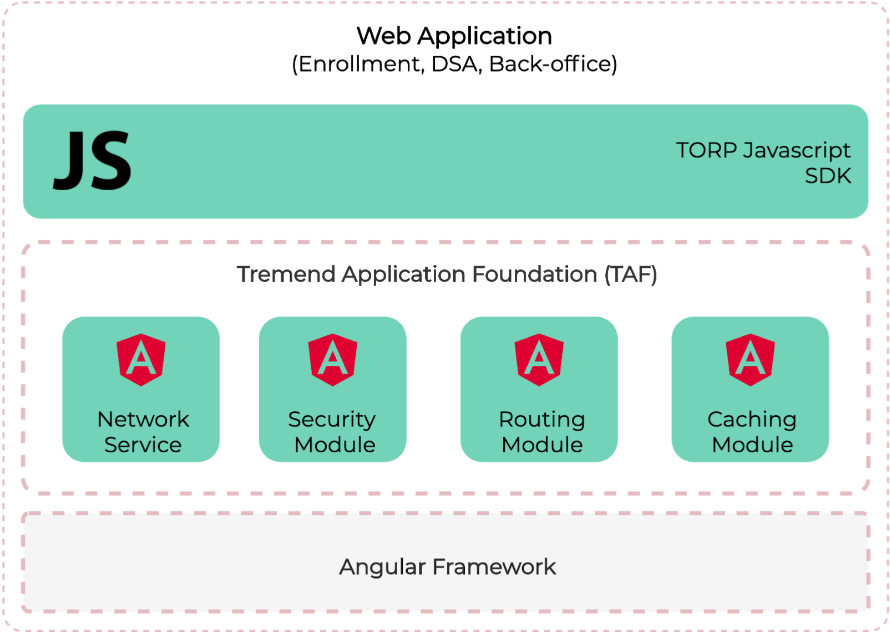


Fig. 2 Technological stack for TORP frontend Applications

TORP Frontend Modules are mostly Angular based, and components from **Tremend Application Foundation** are used. **TAF** packs a collection of libraries and components, out of the box and ready to use in applications that use Angular as UI Framework. The benefits are::

- Reduced development time
- High-quality code-base regarding architecture and technical conventions.
- Multiple plug & play modules: Caching Manager, Network Manager, Database Manager, Deep Linking Navigation, UI Flows (User register flow, user login, platform login) and sample testing specifications.
- The architecture allows for easy modularization, which in turn allows for better testing and the possibility to extract parts of the app into separate apps.

4.3.3.2. TORP Backend Services

Below, the tech stack diagram for TORP Backend Services.

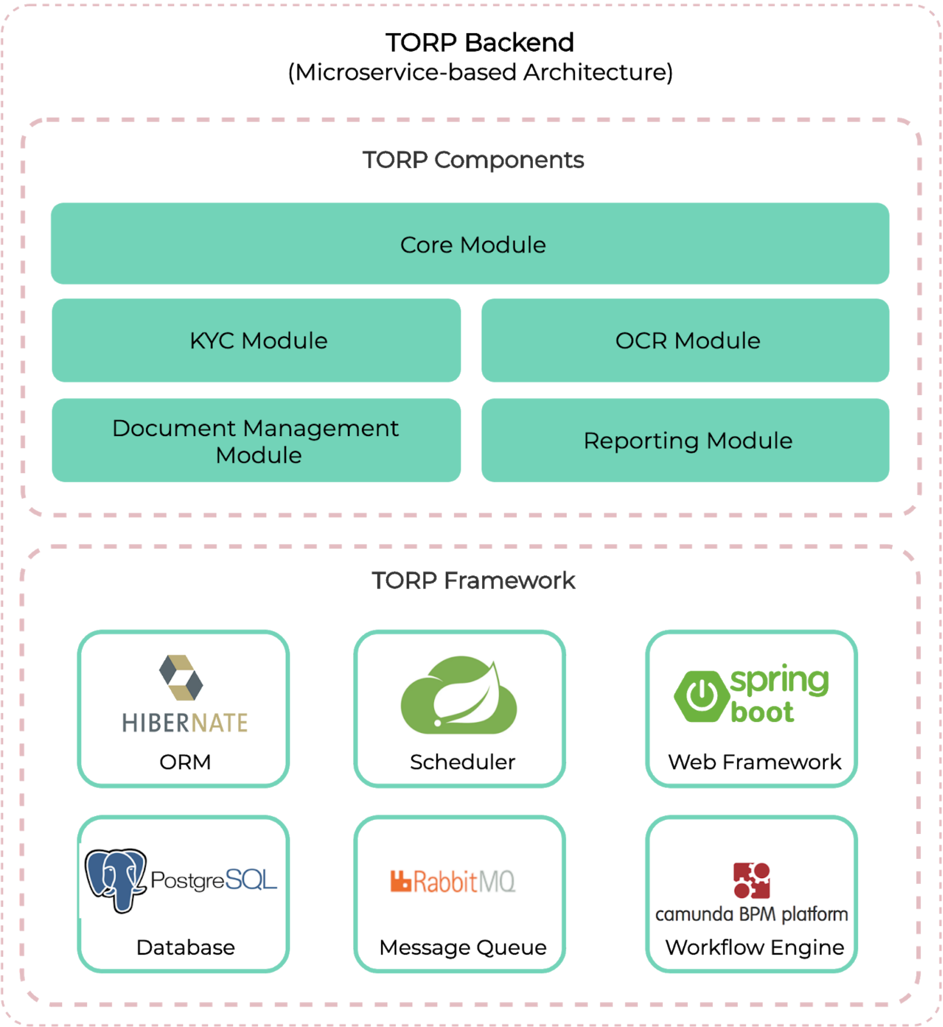


Fig. 3 Tech stack for TORP Back-Office Application

TORP Framework uses PostgreSQL as a database. By employing **Hibernate ORM**, this layer is abstracted and other database engines can be easily plugged-in (MS SQL Server, Oracle DB).

Camunda BPM Platform is used as an engine for workflows. Custom modules are part of the TORP Framework and components and allow integration with 3rd party systems and internal workflows.

The message queue framework of choice for TORP is RabbitMQ. With an MQ in place, TORP ensures maximum availability of the platform during peak times by leveraging workloads evenly.

4.3.4. Deployment network diagram

4.3.4.1. TORP On-Premise model - deployment network diagram

Below you can find a diagram on the proposed TORP on-premise infrastructure, including the role of the software components as well as various integration points with Bank's and 3rd Party services. A hardware replication scenario was also taken into account:

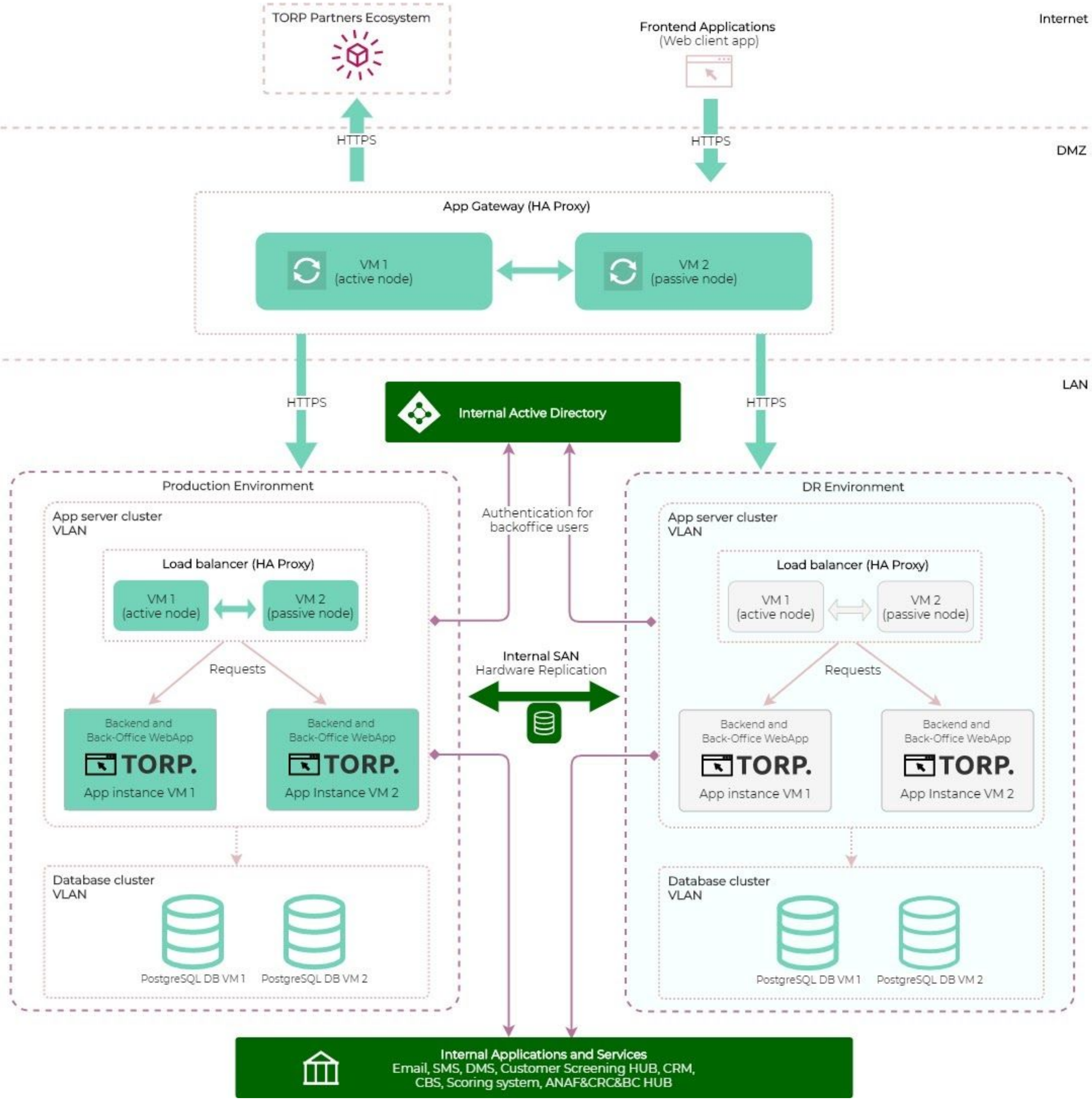


Fig. 4 - On-premise deployment network diagram

4.3.4.2. TORP On-Premise model - Infrastructure Specifications

TORP infrastructure is Virtualization technology and VM’s Operating System agnostic and uses only Open Source software components which, based on Bank's decision, could be upgraded to Enterprise versions.

We propose the following infrastructure specifications based on annual transactional volumes (onboarding & lending):

Option 1. Annual transactions volumes: < 25,000

Role	DEV* & UAT environments	PROD environment	DR environment
App Gateway VM	1 x (1x core, 1GB RAM, 10GB HDD)	2 x (1 x core, 1GB RAM, 10GB HDD)	
Load Balancer VM	1 x (1x core, 1GB RAM, 10GB HDD)	2 x (1x core, 1GB RAM, 10GB HDD)	2 x (1x core, 1GB RAM, 10GB HDD)
App Instance VM	1 x (2x core, 8GB RAM, 30GB HDD)	2 x (4x core, 16GB RAM, 50GB HDD)	2 x (2x core, 8GB RAM, 50GB HDD)
PostgreSQL DB VM	1 x (2x core, 8GB RAM, 100GB HDD)	2 x (4x core, 16GB RAM, 100GB HDD)	2 x (2x core, 8GB RAM, 100GB HDD)
SAN Storage**	100GB	500GB	100GB

Option 2. Annual transactions volumes: between 25,001 and 250,000

Role	DEV* & UAT environments	PROD environment	DR environment
App Gateway VM	1 x (1x core, 1GB RAM, 10GB HDD)	2 x (2 x core, 2GB RAM, 50GB HDD)	
Load Balancer VM	1 x (1x core, 1GB RAM, 10GB HDD)	2 x (2 x core, 2GB RAM, 20GB HDD)	2 x (2 x core, 2GB RAM, 20GB HDD)
App Instance VM	1 x (2x core, 8GB RAM, 30GB HDD)	2 x (6 x core, 32GB RAM, 100GB HDD)	2 x (4 x core, 16GB RAM, 100GB HDD)
PostgreSQL DB VM	1 x (2x core, 8GB RAM, 100GB HDD)	2 x (6 x core, 32GB RAM, 200GB HDD)	2 x (4 x core, 16GB RAM, 200GB HDD)
SAN Storage**	100GB	2TB	300GB

Option 3. Annual transactions volumes: > 250,000

Role	DEV* & UAT environments	PROD environment	DR environment
App Gateway VM	1 x (1x core, 1GB RAM, 10GB HDD)	2 x (2 x core, 4GB RAM, 50GB HDD)	
Load Balancer VM	1 x (1x core, 1GB RAM, 10GB HDD)	2 x (2 x core, 2GB RAM, 20GB HDD)	2 x (2 x core, 2GB RAM, 20GB HDD)
App Instance VM	1 x (2x core, 8GB RAM, 30GB HDD)	4 x (8 x core, 32GB RAM, 500GB HDD)	2 x (8 x core, 32GB RAM, 500GB HDD)
PostgreSQL DB VM	1 x (2x core, 8GB RAM, 100GB HDD)	4 x (8 x core, 64GB RAM, 500GB HDD)	2 x (8 x core, 64GB RAM, 500GB HDD)
SAN Storage**	100GB	4TB	500GB

** DEV Environment will use Tremend infrastructure*

*** SAN Storage requirements will decrease if Bank decides to transfer data to the electronic archive*

4.3.4.3. TORP SaaS model - Cloud deployment network diagram

Please find below a diagram on the proposed Saas model TORP infrastructure using Microsoft Azure Cloud Computing Services, relying on Azure managed services and K8S application cluster high-availability, including also the integration points with Bank's and 3rd Party services:

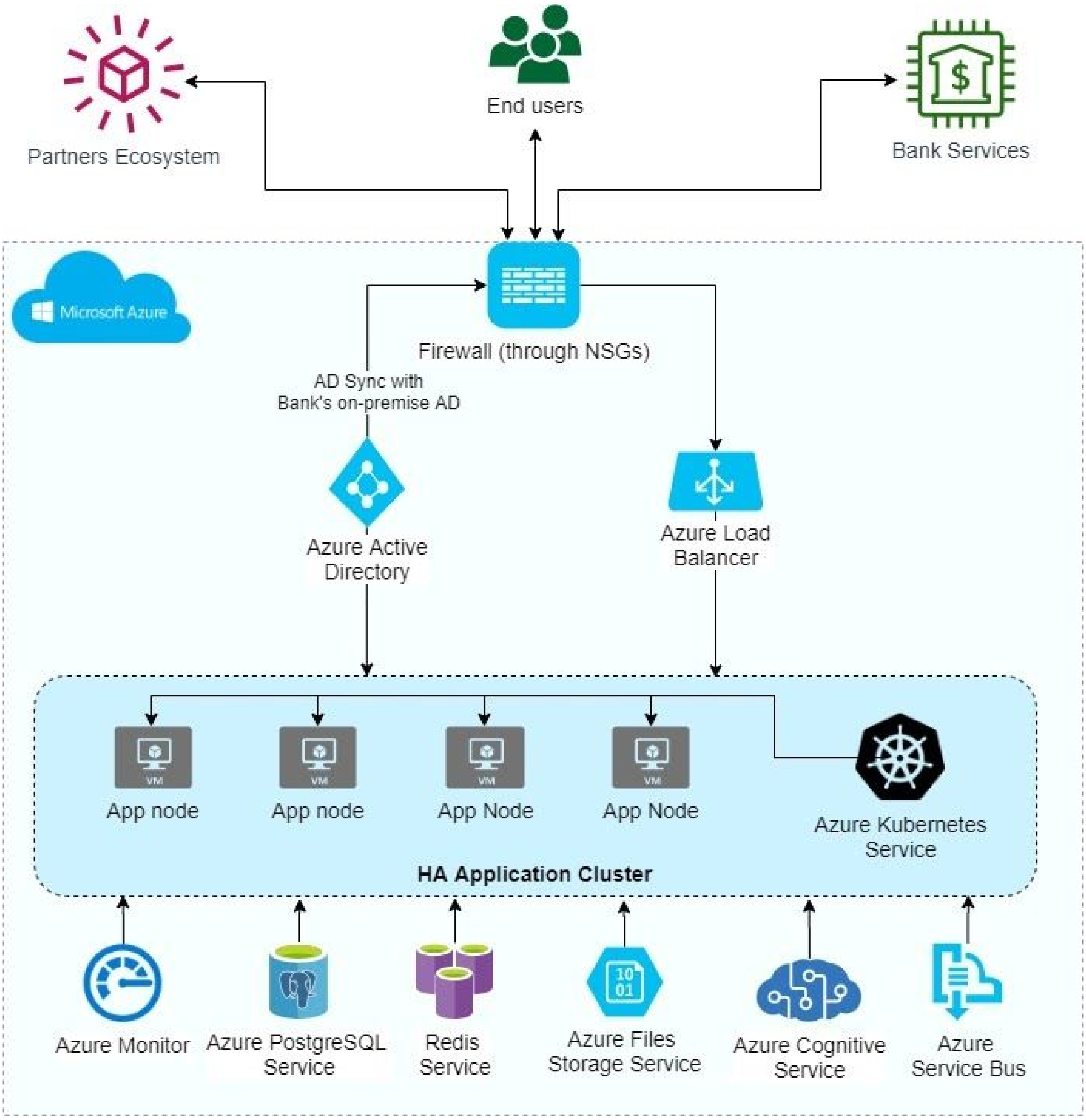


Fig. 5 - Cloud deployment network diagram

The Azure solution deployment will rely on Azure provided managed services for PostgreSQL Database, REDIS cache, shared storage with Azure Files, Azure Monitor for infrastructure and application monitoring, Azure Service Bus for messaging and Azure Cognitive services integrated directly in the solution. The Azure resources and services are resilient to failures, having high-availability and replication as options or directly built-in.

4.3.4.4. TORP SaaS model - Infrastructure Specifications

TORP SaaS model leverage on Microsoft Azure services and, based on Bank's requirements, we propose the following specifications based on annual transactional volumes (onboarding & lending):

Option 1. Annual transactions volumes: < 25,000

Service type	Description
Load Balancer	Standard Tier: 5 Rules, 1,000 GB Data Processed
Bandwidth	Zone 1: North America, Europe, 50 GB
Azure Database for PostgreSQL	Single Server Deployment, General Purpose Tier, 1 Gen 5 (4 vCore), 1 year reserved, 100 GB Storage, 100 GB Additional Backup storage - GRS redundancy
Cognitive Services	Computer Vision: S1 tier, 2000 Tag, Face, GetThumbnail Color, Image Type transactions; 2000 OCR (printed), Adult , Celebrity, and Landmark transactions; 2000 Describe and OCR (handwriting) transactions
Azure Cache for Redis	C1: Standard tier, 1 instance(s), 730 Hours
Service Bus	Standard tier: 1, 1,000 brokered connection(s), 0 Hybrid Connect listener(s) + 0 overage per GB, 0 relay hour(s), 25 relay message(s)
Storage Accounts*	File Storage, Standard Performance Tier, General Purpose V2, LRS Redundancy, 500 GB Capacity, 20 Put or Create Container operations, 20 List operations, 10 Other operations, 0 Additional Sync servers
Azure Kubernetes Service (AKS)	4 D4s v3 (4 vCPU(s), 16 GB RAM) nodes; 3 year reserved; 4 managed OS disks – E4
Azure Monitor	1,010,000 Standard API calls, 4 VM(s) monitored and 10 metric(s) monitored per VM, 16 Log Alert(s) at 5 Minutes Frequency, 101,000 emails, 101,000 push notifications, 1,100,000 web hooks

Option 2. Annual transactions volumes: between 25,000 and 250,000

Service type	Description
Load Balancer	Standard Tier: 5 Rules, 1,000 GB Data Processed
Bandwidth	Zone 1: North America, Europe, 100 GB
Azure Database for PostgreSQL	Single Server Deployment, General Purpose Tier, 1 Gen 5 (8 vCore), 1 year reserved, 200 GB Storage, 200 GB Additional Backup storage - GRS redundancy
Cognitive Services	Computer Vision: S1 tier, 20000 Tag, Face, GetThumbnail Color, Image Type transactions; 20000 OCR (printed), Adult , Celebrity, and Landmark transactions; 20000 Describe and OCR (handwriting) transactions

Azure Cache for Redis	C2: Standard tier, 1 instance(s), 730 Hours
Service Bus	Standard tier: 10, 1,000 brokered connection(s), 0 Hybrid Connect listener(s) + 0 overage per GB, 0 relay hour(s), 250 relay message(s)
Storage Accounts*	File Storage, Standard Performance Tier, General Purpose V2, LRS Redundancy, 2,000 GB Capacity, 200 Put or Create Container operations, 200 List operations, 100 Other operations, 0 Additional Sync servers
Azure Kubernetes Service (AKS)	4 D4s v3 (4 vCPU(s), 16 GB RAM) nodes; 3 year reserved; 4 managed OS disks – E4
Azure Monitor	1,010,000 Standard API calls, 4 VM(s) monitored and 10 metric(s) monitored per VM, 16 Log Alert(s) at 5 Minutes Frequency, 101,000 emails, 101,000 push notifications, 1,100,000 web hooks

Option 3. Annual transactions volumes: > 250,000

Service type	Description
Load Balancer	Standard Tier: 5 Rules, 1,000 GB Data Processed
Bandwidth	Zone 1: North America, Europe, 200 GB
Azure Database for PostgreSQL	Single Server Deployment, General Purpose Tier, 1 Gen 5 (16 vCore), 1 year reserved, 400 GB Storage, 400 GB Additional Backup storage - GRS redundancy
Cognitive Services	Computer Vision: S1 tier, 30000 Tag, Face, GetThumbnail Color, Image Type transactions; 30000 OCR (printed), Adult , Celebrity, and Landmark transactions; 30000 Describe and OCR (handwriting) transactions
Azure Cache for Redis	C3: Standard tier, 1 instance(s), 730 Hours
Service Bus	Standard tier: 19, 1,000 brokered connection(s), 0 Hybrid Connect listener(s) + 0 overage per GB, 0 relay hour(s), 349 relay message(s)
Storage Accounts*	File Storage, Standard Performance Tier, General Purpose V2, LRS Redundancy, 4,000 GB Capacity, 300 Put or Create Container operations, 300 List operations, 150 Other operations, 0 Additional Sync servers
Azure Kubernetes Service (AKS)	4 D8 v3 (8 vCPU(s), 32 GB RAM) nodes; 3 year reserved; 4 managed OS disks – E6
Azure Monitor	1,010,000 Standard API calls, 4 VM(s) monitored and 10 metric(s) monitored per VM, 16 Log Alert(s) at 5 Minutes Frequency, 101,000 emails, 101,000 push notifications, 1,100,000 web hooks

** Azure Storage requirements will decrease if Bank decides to transfer data to the electronic archive*

4.3.4.5. Interfaces with Bank's Services

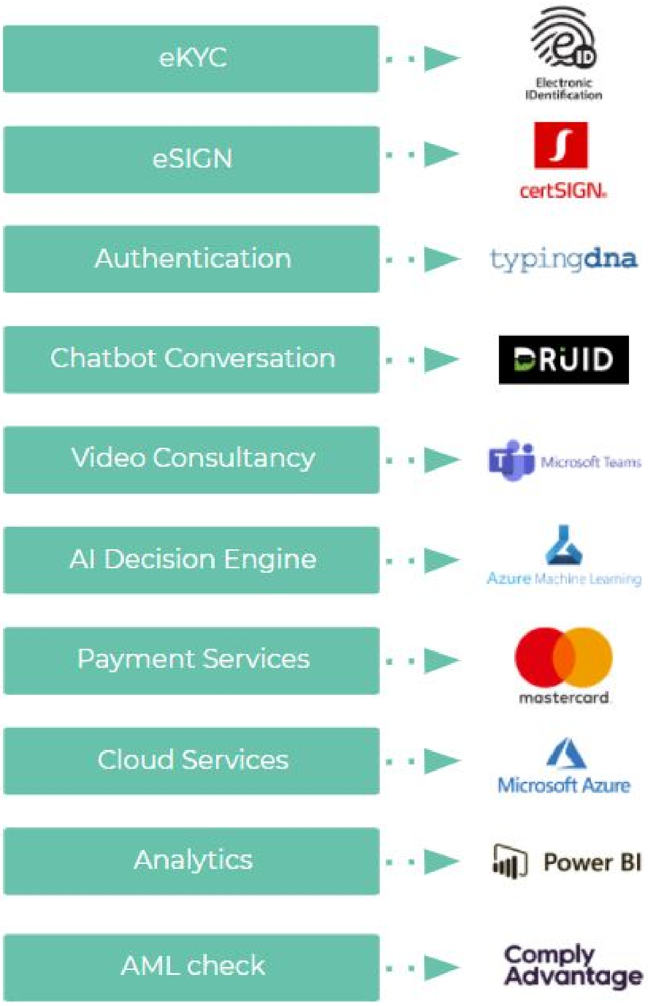
According with Bank's requirements, TORP can be interfaced with the following Bank applications and services:

- Active Directory services - back-office users authentication
- E-mail services - internal and external email notifications;
- SMS delivery services - internal and external SMS notifications (e.g. One Time Password);
- Scoring System - for risk profile calculation;
- Document Management System;
- Customer Screening services;
- ANAF & CRC & BC HUB;
- CRM/ERP/Core Banking System.

4.3.4.6. TORP Partners Ecosystem Services

TORP relies on Tremend Application Foundation (TAF) Open API-based interface layer, making it seamlessly pluggable with our Partner's solution, 3rd party service or any existing in-house infrastructure.

Depending on the Financial Institution selected infrastructure model (on-premise or Cloud SaaS) and on the required functionality set, TORP relies on the best-of-breed Partner ecosystem, providing out-of-the-box interfaces with the following fintech services:



4.3.4.7. Interfaces with core eKYC and eSIGN Services

1. **Microsoft Cognitive Services -** light customer identification

   In the On-Premise scenario, TORP is interfaced with Microsoft Cognitive SaaS for executing the customer initial identification. The integration relies on APIs and performs the following processes: Romanian ID Cards OCR, face recognition & comparison between customer uploaded photo (selfie) and ID Card picture and liveness detection. The Cognitive Cloud Computing Services location is European Union (Leopardstown, Dublin, Ireland).

2. **ElectronicID** (eID) **-** biometric video identification

   eID Service represents a global standard remote identification solution based on the strongest level of compliance with the most strict European regulations and supports several Electronic Identification Services.
   The integration between TORP and eID SaaS relies on APIs and supports the following electronic identification equipment: smartphones (Android and IOS) and desktops with a video camera and an internet browser. An isolated eID instance will be instantiated for the FI, leveraging on AWS Cloud Computing Services located in European Union (Clonshaugh Road, Clonshagh, Dublin 17, Ireland).

3. **CertSIGN** - digital certificate issuance, electronic signature and electronic archival services

   CertSIGN is the first Romanian Company to offer remote electronic signature certified at European level.

   TORP is interfaced with CertSIGN SaaS through APIs for providing the following services:

   - Qualified, advanced and simple **digital certificates** issued according to EU eIDAS Regulation 910/2014;
   - Remote qualified **electronic signature** creation service (Paperless) certified according to EU eIDAS Regulation 910/2014 as Remote Qualified Electronic Signature Creation Device, both software and hardware;
   - **Electronic documents archiving** services with legal value in accordance with Romanian law 135/2007.

   These services are delivered from CertSIGN authorized Data Center located in Bucharest, Romania.

05. **TORP.** Subcontracted Services

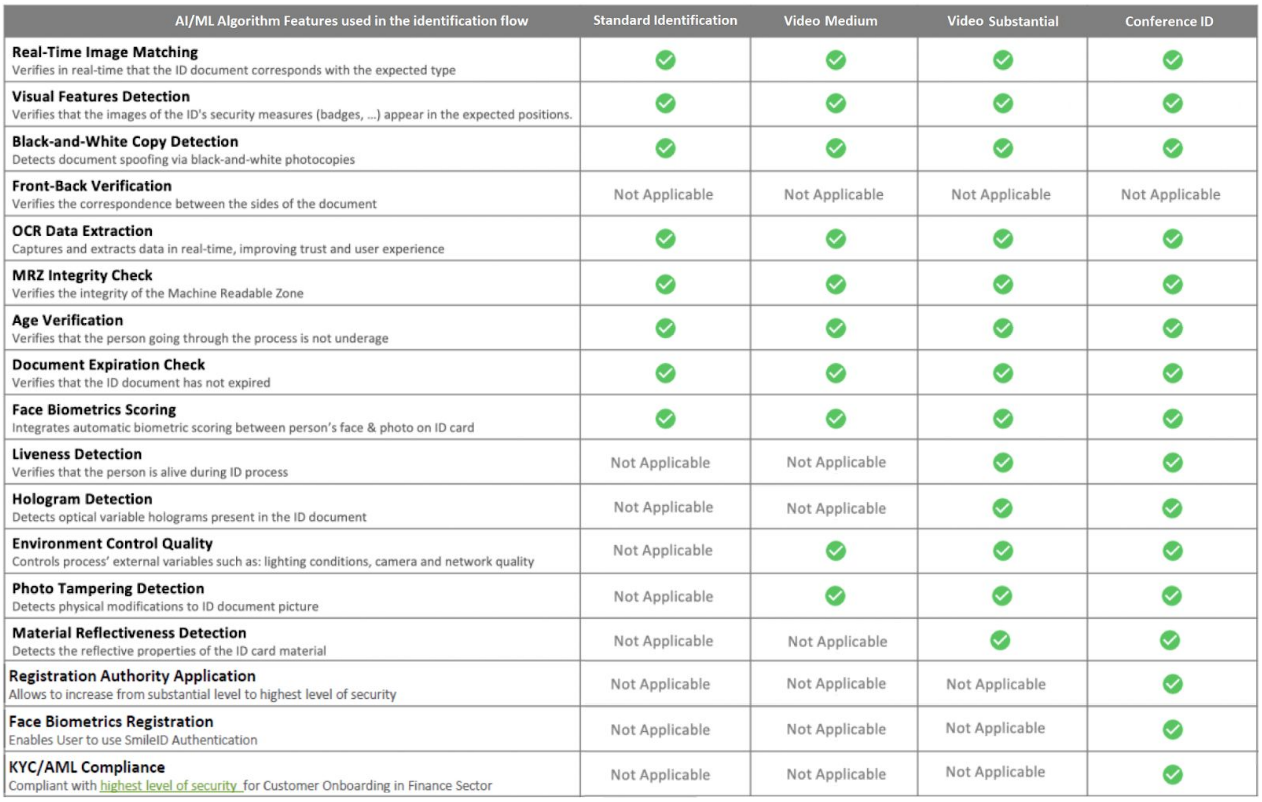
5.1. Electronic Identification S.L. - Remote Customer Identification

In order to perform the remote customer identification process used in the COM - Customer Onboarding Module (Building Blocks: "ID Card scan & OCR" and "Biometric Video Identification"), TORP is interfaced with an external service provided by ELECTRONIC IDENTIFICATION S.L., the Licensor Subcontractor, identified as follows:

> **ELECTRONIC IDENTIFICATION S.L.** (hereinafter, **eID)**, with address at Madrid Avenida Ciudad de Barcelona, 81-A, floor 4, 28007 Madrid, SPAIN, constituted by public deed granted before the Notary of Madrid, Mr Emilio Leal Labrador on July 7, 2016, with protocol number 1,300 and registered in the Mercantile Registry of Madrid in Volume 30,920, Page 153, Section 8, Page M-556508 and Registration 7, CIF B-86681533.

The integration between TORP and eID service relies on APIs and supports the following electronic identification equipment: smartphones (Android and IOS) and desktops with a video camera and an internet browser.

eID Service represents a global standard remote identification solution based on the strongest level of compliance with the most strict European regulations and supports several Electronic Identification Services, with different levels of security:



AI/ML Algorithm Features used in the identification flow	Standard Identification	Video Medium	Video Substantial	Conference ID
Real-Time Image Matching Verifies in real-time that the ID document corresponds with the expected type	✓	✓	✓	✓
Visual Features Detection Verifies that the images of the ID's security measures (badges, ...) appear in the expected positions.	✓	✓	✓	✓
Black-and-White Copy Detection Detects document spoofing via black-and-white photocopies	✓	✓	✓	✓
Front-Back Verification Verifies the correspondence between the sides of the document	Not Applicable	Not Applicable	Not Applicable	Not Applicable
OCR Data Extraction Captures and extracts data in real-time, improving trust and user experience	✓	✓	✓	✓
MRZ Integrity Check Verifies the integrity of the Machine Readable Zone	✓	✓	✓	✓
Age Verification Verifies that the person going through the process is not underage	✓	✓	✓	✓
Document Expiration Check Verifies that the ID document has not expired	✓	✓	✓	✓
Face Biometrics Scoring Integrates automatic biometric scoring between person's face & photo on ID card	✓	✓	✓	✓
Liveness Detection Verifies that the person is alive during ID process	Not Applicable	Not Applicable	✓	✓
Hologram Detection Detects optical variable holograms present in the ID document	Not Applicable	Not Applicable	✓	✓
Environment Control Quality Controls process' external variables such as: lighting conditions, camera and network quality	Not Applicable	✓	✓	✓
Photo Tampering Detection Detects physical modifications to ID document picture	Not Applicable	✓	✓	✓
Material Reflectiveness Detection Detects the reflective properties of the ID card material	Not Applicable	Not Applicable	✓	✓
Registration Authority Application Allows to increase from substantial level to highest level of security	Not Applicable	Not Applicable	Not Applicable	✓
Face Biometrics Registration Enables User to use SmileID Authentication	Not Applicable	Not Applicable	Not Applicable	✓
KYC/AML Compliance Compliant with highest level of security for Customer Onboarding in Finance Sector	Not Applicable	Not Applicable	Not Applicable	✓

5.2. **CertSIGN S.A.** - Digital Certificate, eSignature and eArchive

In order to perform the digital certificate issuance and the electronic signature for the processed documents, using a trust services compliant with European and Romanian legislation, in the COM - Customer Onboarding Module (Building Blocks: "ID Card scan & OCR" and "Biometric Video Identification"), TORP is interfaced with an external service provided by CertSIGN, the Licensor Subcontractor, identified as follows:

> **CertSIGN S.A.** (hereinafter, **certSIGN)**, with address at Bd. Tudor Vladimirescu nr. 29 A AFI Tech Park 1, Sector 5, București, România, Nr.Reg.Com.: J40/484/2006, fiscal registration ID: RO18288250

CertSIGN is a company based in Romania, specialized in developing information security software applications and providing services related to the protection of information and information systems in almost 20 countries worldwide. TORP CertSIGN services:

- Human **operator assistance** during the remote customer video identification
- Qualified, advanced and simple **digital certificates** issued according to EU eIDAS Regulation 910/2014;
- Remote qualified **electronic signature** creation service (Paperless) certified according to EU eIDAS Regulation 910/2014 as Remote Qualified Electronic Signature Creation Device, both software and hardware;
- **Electronic documents archiving** services with legal value in accordance with Romanian law 135/2007.

5.2.1. eIDAS Qualified trust services

Remote signing solution

This scenario involves providing a Paperless service for remote qualified electronic signature creation based on a remote issuance of the qualified digital certificates in accordance with eIDAS Regulation 910/2014 and the best practices related to electronic signature.

Legal context

CertSIGN provides qualified digital certificates compliant with „eIDAS Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC'' and with Romanian legislation MCSI (Minister for Communications and Information Society) Order no. 449/2017 „On the procedure for granting, suspending and withdrawing the qualified trust service provider status in accordance with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014”.

eIDAS Regulation 910/2014 describes the remote signature as being a service which can be provided only by a Qualified Trust Service Provider (QTSP) taking into consideration a mechanism which assures the sole control of the signatory to its private key.

- eIDAS 910/2014 (Recital 52) “*In order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that* ***the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply”.***

Therefore, for complying with eIDAS Regulation, a Remote solution for QES has to be audited and certified in terms of:

- specific management and security procedures;
- trustworthy software;
- hardware and secured electronic communication channels.

This certification shall assure the sole control of the signatory for the remote signature creation environment. In case of litigation, it is proven that the signatory has signed the electronic documents.

Moreover, in order to create Qualified Electronic Signatures, the remote signing solution must be a QSCD. To fulfil this legal requirement certSIGN proposes its Paperless solution that is certified as a Remote QSCD and present on the EU list of Qualified Signature creation devices:

https://ec.europa.eu/futurium/en/system/files/ged/eidas-art.31-list-2019-06-03.pdf

General description

CertSIGN proposes its own, eIDAS certified, Remote Qualified Electronic Signature solution provided as a service with the following components:

- Signing Service Application (SSA) – the basic component of the system that stores user certificates and is used to create an electronic signature and add a timestamp to documents and hashes;
- CA Service – a service that has the role of transmitting certificate requests to Certification Authority;
- Authorization mechanisms (e.g. SMS, e-mail, biometrics) – used to authorize the signature process and to ensure the customer's sole control of its private key within the ecosystem;
- HSM – a cryptographic hardware device used that stores the private keys, certified also as QSCD according to eIDAS Regulation.
- Client application for hash calculation and PDF signature embedding.

The service implements a remote signing mechanism based on qualified digital certificates issued according to eIDAS Regulation 910/2014 and an audited environment for remote qualified signature creation in which the private keys of the user will be stored on a QSCD certified cryptographic device.

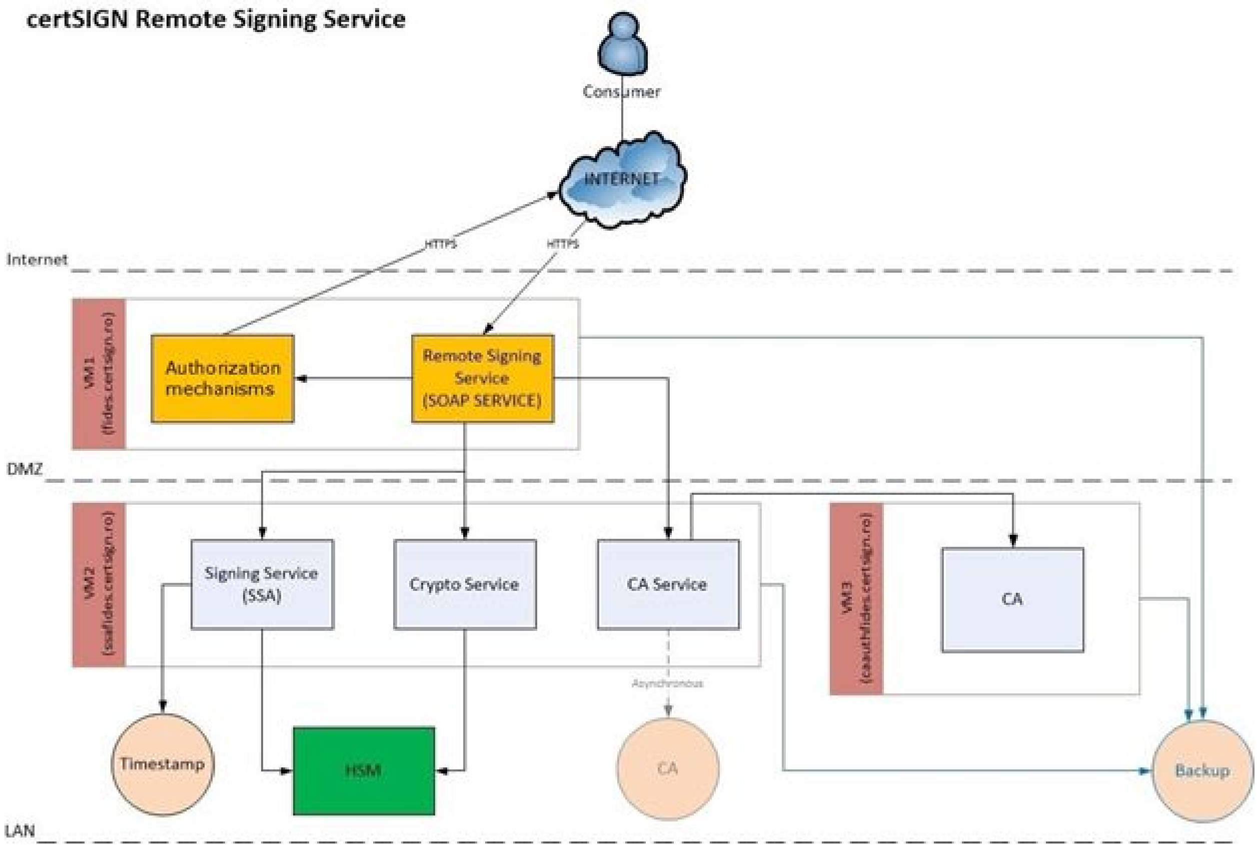
System overview

Paperless Remote QES works on a client-server architecture, running as a web service on a Windows platform hosted in Internet Information Services (IIS). To create digital signatures, Paperless Remote QES uses a hardware security module (nShield HSM, accredited as QSCD).

The basic component is a web service developed in WCF (Windows Communication Foundation), exposed by the SOAP protocol through HTTPS and is running as a web application in IIS (Internet Information Services). The component is deployed in a distributed architecture to ensure high performance and security.

To issue qualified digital certificates, certSIGN Paperless has the functionality to generate the private cryptographic key on a QSCD HSM and the certificate request (PKCS#10) for the digital certificate that will be used to sign documents and hashes. After that, the signing service communicates with the Certification Authority (CA), by retransmitting the certificate request and user information. The certificate request will also contain the ***validity of the certificate (e.g. 1 hour, 24 hours, up to three years)***, which can be up to three years.

The Certification Authority will issue qualified digital certificates that will be used to sign documents and hashes, according to that data.



The system has been designed and implemented in a modular way so that its customer's client platform can interact with it through various standardized methods and technologies:

- Mobile applications, installed on iOS or Android;
- Web applications;
- Integration with client's existing systems and infrastructures.

Another component of the system is the Time Stamping Authority that will provide time-stamping service for the signature applied to the documents and hashes. Timestamps are issued by certSIGN, qualified trust service provider for issuance of qualified time stamps, according to eIDAS Regulation 910/2014.

Main functionalities for project implementation

The paperless solution will allow, remotely, qualified digital certificate issuance and qualified electronic signature creation so that could cover all signing functionalities requested in the Project:

- **Customer:**
  - Certificate dynamic validity: one-shot, 1 hour, 1 month, up to three years;
  - Digital certificate issuance for simple, advanced and qualified electronic signature;
  - Allows single document and batch documents signing;
  - Authorization mechanism – OTP (via SMS, e-mail), TORP biometrics, etc.

- **Bank employee:**
  - Certificate validity: one-shot, 1 hour, 1 month, up to three years. We recommend using long term validity certificates for employees;
  - Allows single document and batch documents signing (automatically or configurable authorization timeframe);
  - Electronic archive access in order to check electronically signed documents.

Security

Providing qualified trust service according to national and European legislation has conducted a set of certain physical and practical security measures. All personnel involved in providing qualified trust services have its role and is acting within a secured and audited ecosystem.

Site location and environment

All CertSIGN operations are conducted within a physically protected environment with controls based on the risk assessment that is meant to deter, prevent, detect and counteract the materialization of risks on its assets. We also maintain disaster recovery facilities for our CA and RA operations, facilities that are protected by physical security controls similar to those implemented at our primary facility. All physical security controls implemented by CERTSIGN are in accordance with ISO 27001 and 27002 standards and are described in detail in the security policies and procedures.

The most important security controls are:

- A clearly defined and protected perimeter through which all entries and exits are monitored;
- Critical components are protected with several perimeters;
- An access control system configured to allow access only to those individuals appropriately cleared and specifically authorized to enter the area;
- Manned and electronic monitoring for unauthorized intrusion at all times;
- Personnel not on the access list are properly escorted and supervised;
- A site access log is maintained and inspected periodically;
- Every piece of equipment is correctly maintained to ensure its continuous availability and integrity.

Trusted Roles

A number of audited Roles are managing the environment responsible for the Registration Authority and Certification Authority for enrolling certificate requests and issuing qualified digital certificates. Some of the Roles are described below:

Security officer – Overall responsibility for the implementation of security practices and policies.

System administrator – Authorized to install, configure and maintain the Certification Authority's trustworthy systems for registration, certificate generation, subject device provision and revocation management. Installs hardware and operating systems; installs and configures the network equipment.

System operator – Responsible for operating the Certification Authority's trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Has access to Subjects' certificates; revokes Subjects' certificates; provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subjects/ Subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies to the designated premises.

Registration Officers: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests;

Revocation Officers: Responsible for operating certificate status changes;

System Auditor – Authorized to access archives and audit logs of the Certification Authority's trustworthy systems. Responsible for the performance of internal audit, compliance of a Certification Authority with this CPS; this responsibility extends also to the Registration Authority, operating within CERTSIGN.

The role of the auditor cannot be combined with any other role in CERTSIGN. No entity having assigned any other role different than an auditor may take auditor's responsibilities. Employees are formally appointed to trusted roles by the Policies and Procedures Management Body (PPMB). The "least privilege" principle is applied when assigning access rights to trusted roles.

Each CERTSIGN employee acting in a **trusted role** is identified and authenticated to access the infrastructure to conduct his role by means of at least 2 factors authentication credentials.

Every assigned account:

- Is unique and directly assigned to a specific person,
- Is not shared with any other person;
- Is restricted according to function (arising from the role performed by a specific person) based on the CERTSIGN software system, operating system and application controls.

All actions of employees in trusted roles are traceable and full accountability is ensured.

Traceability, logging and proofs for trust services providing

Each operation related to a client enrolment, qualified certificate issuance, revocation or expiration is subject to an audited process implemented within RA and CA infrastructure. Every critical activity from CERTSIGN's security point of view is recorded in event logs and archived. CERTSIGN event logs contain recordings of all activities generated by the software components within the system.

These recordings are divided into three distinct categories:

System logs – contain information about customer's requests and server's responses (or vice versa) at the level of the network protocol (for example HTTP, https); the recorded data is: IP address of the station or server, performed operations (for example searching, editing, writing, etc.) and their results (for example the successful entry of a record in the database);

Errors – contain information about errors at the network protocols level and at the applications' modules level;

Audit logs – contain information specific for the certification services, for example, registration and certification request, rekey request, certificate acceptance, certificate issuing, and CRL, etc. The above logs are common to every component installed on a server or on a workstation and have a predefined capacity. When this capacity is exceeded a log version is automatically created.

Every automatic or manual recording contains the following information:

- Event type;
- Event identifier;
- Date and time of the event occurrence;
- Identifier of the person in charge of the event.

All events relating to the life-cycle of CA keys are recorded.

All events relating to the life-cycle of certificates are recorded.

All events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA are logged.

All requests and reports relating to revocation, as well as the resulting action are logged. All events related to registration including requests for certificate re-key are logged.

All registration information, including the following, is recorded:

- Type of document(s) presented by the applicant to support registration;
- Record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
- The storage location of copies of applications and identification documents, including the signed Subject/ Subscriber agreement;
- Any specific choices in the Subject/ Subscriber agreement (e.g. consent to the publication of certificate);
- Identity of entity accepting the application;
- The method used to validate identification documents.

In addition, CertSIGN maintains internal logs of all security events and all relevant operational events in the whole infrastructure whatever the component service, including, but not limited to:

- Changes to the security policy;
- Start and stop of systems;
- Outages;
- System crashes and hardware failures;
- Firewall and router activities;
- PKI system access attempts;
- Physical access of personnel and other persons to sensitive parts of any secure site or area;
- Back-up and restore;
- Report on disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Access to logs is exclusively allowed for the security officer, specially appointed personnel, and auditors. The privacy of subject information is maintained.

Security of the Remote QES service

The information system that ensures the functionalities of remote signing solution is secured 360 degrees, as follows:

- It is hosted in certSIGN data centre, which has all the physical security elements at “state-of-art” level:
  - Access control;
  - Power supply redundancy;
  - Fire extinguishing system;
  - Air conditioning system;
  - Anti-flood system;
  - Video monitoring system;
  - Redundant connections using two Internet Service Providers;
- Logical security provided by a cluster of NGFW (next-generation firewall) equipment with IDS and network antivirus functionalities;
- The processing system is configured in active-active cluster mode with load balancing;

- The systems are hardened from configurations point of view;
- The systems are accessible to administrators through PAM (Privileged Access Monitoring) solutions;
- The entire infrastructure is monitored in 24x7 mode from the Security Operation Centre operated by certSIGN:
    - Operational monitoring (via SNMP):
        - The services are functional;
        - The network equipment is functional;
        - The processing systems are functional;
        - The services are accessible from the Internet
        - Management of equipment and systems configurations
        - Personalized alerts on alternative channels in case of an operational incident (email, SMS)
    - Security monitoring:
        - Dedicated CSIRT team
        - The logs of the equipment, systems and services in the infrastructure are collected, analysed and correlated in a SIEM solution;
        - Personalized alerts in case of security incidents;
        - Regular scanning from the point of view of information vulnerabilities and patch management;
        - Solution for ensuring the integrity of the configuration files;
        - Periodic pentest.
- The proposed technical solution is certified as QSCD at Eu level
- The implementation of the technical solution was audited and it was declared compliant with the eIDAS Regulation requirements for the creation of QES.

5.2.2. Electronic archiving services

General description

certSIGN proposes an electronic archiving solution that consists of electronic archiving of electronically signed documents in accordance with the requirements of:

- Law No. 135 / 2007 regarding archiving documents in electronic form;
- MCSI Ministerial Order no. 493/2009 on technical and methodological rules for the application of Law no. 135/2007 on archiving electronic documents;
- MCSI Ministerial Order no. 489 / 15.06.2009 regarding the methodological norms for the authorization of data centres.

The electronic archiving solution is designed in accordance with the best practices and simplifies the storage of documents, bringing a large number of benefits to the Bank.

Electronic archive description

The collected data will be electronically archived within the integrated electronic archiving platform.

The process of storing the electronically signed documents in the archive will be done through a dedicated service that automatically takes the documents and inserts them in the electronic archive.

certSIGN is authorized as an electronic archive administrator and also has its own data centre authorized by the Ministry of Communications and Information Society (MCSI) according to the existing legal framework. The process of retrieval, storage and delivery of documents in and from the electronic archive is done through a secure archiving application, accessible at http://e-arhivare.certsign.ro.

06. **TORP.** Maintenance and Support services

Tremend is fully committed to respecting the Service Levels and metrics presented below, for TORP components and for all 3rd party services:

- **ElectronicID:** Remote Customer Video Identification service
- **CertSIGN:**
    - Qualified digital certificate issuance service
    - Electronic Signature service
    - Human agent assistance during the video identification
    - Electronic Archival service

6.1. Service Level Agreement

- Service delivery timeframe: 24*7;
- Operational support delivery timeframe: Mo-Fr 09:00-18:00;
- Core eKYC & eSIGN services availability SLA:
    - **eKYC** - Remote Customer Identification: 99.9%
    - **eSIGN** - Electronic Signature: 99.00%
- TORP SaaS model delivers the following SLA, relying on the Azure Managed Services built-in failure resilience, high-availability and replication features, and on Database layer's Geo-Redundant Backup architecture:
    - Availability: 99.9%;
    - RPO = 1 hour;
    - RTO = 12 hours
- Issues definition:

Level	Definition
P1 - Critical issue	The critical error that completely disables the operation of the product, for which there is no solution and has a clear and significant impact on the client's operations.
P2 - Medium priority issue	Serious error for which there is an alternative or non-critical error that significantly affects the functionality of the service and the production.
P3 - Common issue	The isolated error does not significantly affect the functionality of the service.

- Response and Resolution times:

Level	Standard Response Time	Maximal Response Time	Standard Resolution time	Maximal Resolution time
P1	1 hour	2 hour	8 hours	16 hours
P2	4 hours	6 hours	24 hours	32 hours
P3	8 hours	16 hours	48 hours	72 hours

Tremend offers a wide area of standard service, for all support levels:

- **Level 1 -** Technical support (phone and email) in charge with customer's requests, ticket evaluation and resolution
    - Service delivered by Tremend.
- **Level 2 -** Technical support (phone and email) for troubleshooting in terms of service dysfunctionalities and resolution
    - Service delivered by Tremend and its subcontractors (ElectronicID and CertSign)
- **Level 3 -** Technical support (phone, email, on-site) in charge of research and development analyses, architectural updates, upgrades and security deployments
    - Service delivered by Tremend and its subcontractors (ElectronicID and CertSign)

6.2. TORP On-Premise model - remote access requirements

In order to comply with the aforementioned SLA, the Bank must grant the following remote access types to Tremend technical team for support/troubleshooting:

- read-write access, during the pre-UAT & UAT phases, in UAT environment, both application and database layers, on both DMZ and LAN VNETs;
- on a need basis, read-only access in Production environment, both application and database layers, on both DMZ and LAN VNETs.

For the above access we recommend a VPN secure connection through SSH or RDP via a restricted jump server for access exclusively to the solution infrastructure. If for the Production environment such setup is not possible, we can agree on a more restricted access procedure involving screen-sharing of a Client's system administrator connection to the environment and granting session control for executing commands on the infrastructure - although such a procedure will involve Client's personnel availability during Tremend access.

6.3. TORP SaaS model - system operations and maintenance services

If the Bank selects the SaaS model, the system operations and maintenance services for TORP's Azure Infrastructure will be delivered by Tremend DevOps team, which will provide the following services:

- Weekly monitoring - checks of backup existence and consistency and checks for patches availability for the system components
- Identification of necessary maintenance windows (system downtime)
- Daily monitoring of infrastructure health indicators (CPU, MEM and Disk usage, Network traffic) and investigations of the alerts received from the monitoring system
- Corrective actions when required, based on the above monitoring tasks:
    - Scale resources or auto-scaling rules adjustments for accommodating increased/decreased usage and performance baseline re-alignment;
    - Backup files management;
    - Maintenance windows planning and execution;
    - Patches and updates application.

TORP Infrastructure monitoring is provided through Azure Monitor, which will be configured for:

- Kubernetes cluster nodes monitoring - currently proposed 4 VMs, but for increased resource allocation (more VMs) the monitoring will cover all of them
- 10 metrics monitored per VM
- Azure services monitoring - Azure PostgreSQL, Redis, Azure Service Bus and the Azure Storage account
- 16 log signals monitored and queried every 5 minutes
- Alerting through emails, webhooks and push notifications (100K threshold)
- Logs analytics - for detailed logs availability and analysis, with 6 months retention (configurable)

We are proposing a very flexible backup and restore facilities, using the Azure Platform capabilities which backups on 2 levels:

- **Database backup -** performed automatically, with Geo-Redundancy Storage.
  We propose a standard backup flow, with weekly full backups and twice a day differential backups for servers (max supported storage of 4 TB). Snapshot backups happen at least once a day for servers that support up to 16 TB of storage. Transaction log backups in both cases occur every five minutes. The first snapshot of full backup is scheduled immediately after a server is created. The initial full backup can take longer on a large restored server. The earliest point in time that a new server can be restored to is the time at which the initial full backup is complete. As snapshots are instantaneous, servers with support up to 16 TB of storage can be restored all the way back to the creation time.
  More details here: https://docs.microsoft.com/en-us/azure/mysql/concepts-backup

- **Virtual machine backups -** Azure Backup provides independent and isolated backups to guard against accidental destruction of original data. Backups are stored in a Recovery Services vault with built-in management of recovery points. Geo-redundant Storage (GRS) replicates your data to another data center in a secondary region, but that data is available to be read only if a failover is initiated from the primary to secondary region. For a storage account with GRS enabled, all data is first replicated with locally redundant storage (LRS). An update is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region using GRS. When data is written to the secondary location, it's also replicated within that location using LRS.
  More details here: https://docs.microsoft.com/en-us/azure/backup/backup-overview

07. **TORP.** Partners accreditations

–

7.1. eKYC - Electronic Identification

1. **New eIDAS European Regulation 910/2014**: eIDAS regulates levels of security in electronic identification and rest of eTrust Services

2. **European AML5 AntiMoney Laundering**: Client non-presential relationships - eID Kit AML® enable organizations to adopt new KYC European Authorizations

3. **European General Data Protection Regulation (GDPR)**: The most important change in data privacy regulation in 20 years which replaces the Data Protection Directive 95/46/EC

4. **Electronic Administration**: New administrative procedures regulation allowing electronic means and e signature to citizenship relationships as 39/2015

5. **Telecommunications directive 2006/24/CE**: For Secure Societies purposes and fraud prevention

7.2. eSIGN - CertSIGN

1. Qualified Trust Service Provider in accordance with eIDAS Regulation 910/2014 for the following qualified trust services (https://webgate.ec.europa.eu/tl-browser/#/tl/RO/2) :
    - Qualified digital certificates for electronic signatures;
    - Qualified digital certificates for electronic seals;
    - Qualified time-stamping services;
    - Qualified digital certificates for websites EV-SSL;

2. Qualified certificates for electronic signature service Provider in accordance with Romanian legislation no. 455/2001 - https://www.comunicatii.gov.ro/wp-content/uploads/2018/08/Registrul-Furnizorilor-de-Servicii-de-Certificare-1.pdf

3. Paperless QSCD software and hardware certified for remote creation of qualified electronic signature - https://ec.europa.eu/futurium/en/system/files/ged/eidas-art.31-list-2019-08-01.pdf;

7.3. eArchive - CertSIGN

1. Providing electronic archiving services in accordance with law no. 135/2007 - https://www.comunicatii.gov.ro/wp-content/uploads/2018/08/REGISTRU-ARHIVE-ELECTRONICE-.pdf

08. Delivery Methodology

–

8.1. Agile Delivery Methodology

The project is most suitable to be developed using an Agile approach, iteratively using the following key software delivery principles:

- Frequent fully functional releases;
- Automated end-to-end release processes, testing, and multi-staged delivery;
- Version control policies;
- Code reviews and pulls requests;
- Well established Definition of Done & Definition of Ready for user stories, epics and sprints.

The suggested project approach is to accommodate the **Agile principles** to the project-specific context, with a custom tailoring of the applied processes so that they meet the project needs. Actual and further development of requirements will be prioritized to build a realistic roadmap and then planned to be implemented in future releases, according to the mutually agreed-upon roadmap.

We propose **Scrum** as the development methodology of choice for this project, with a one week Discovery phase. The purpose of the Discovery phase is to high-level identify all features and to assess them in terms of size, priority, and dependencies, with the Business Analyst in the team and the Product Owners.

Releases will be made every sprint in a non-production environment, and the work done will be demoed to Bank's stakeholders to be accepted in accordance with the Definition of Done established for each item (story/ sprint/ release).

Two major production releases are scheduled during development and migration phase:

- MVP Deployment
- Data migration and security updates

Minor releases will be scheduled during warranty and maintenance phases for any incident requiring technical support. For **maintenance** period we propose a **Kanban** approach which is suitable for Support Services since it provides the right level of agility required. Priorities and releases are reviewed on a daily basis, according to the severity of the issues raised.

In terms of **project communication management**, regular meetings will be scheduled both internally with the team members and directly with the appropriate Bank's stakeholders.

The frequency of the proposed meetings highly depends on how the project evolves, but initially, we would suggest the following:

- Team ceremonies: every week/ every sprint;
- A steering committee with the client: one sync meeting per sprint.

.

You can also check Tremend's Software Development Life Cycle here:

Tremend Methodology - 01. SDLC.pdf

8.2. Testing and automation

The development of the tests shall be aligned with the standard Tremend QA process which is a time-tested methodology. The QA Engineer will write test cases in Testrail based on the User Acceptance Criteria and will execute a requirements traceability matrix report, to ensure that all stories are covered by the test cases.

Each test case shall be marked with a priority level, and each intermediate release will be tested against the Blocker priority test cases, in addition to the test cases for the delivered functionality. Major releases will have a full regression test suite run. To test the current application, we will perform functional and non-functional tests.

The main goal of TORP integration and customization testing is to ensure that the end2end customer identification and lending flows, as well as the back-office administration modules, works as intended.

We will ensure that TORP interfaces with the Bank systems and external interfaces (ANAF, Credit Bureau) will not affect any functionality of the base product. Functional tests will focus on API tests and UI Tests.

Functional tests will cover scenarios such as the following:

- Verify that the National Agency for Fiscal Administration and Credit Bureau data integrity. For this we will define a JSON Schema or XML Schema (depending on the type of API) and check the received data against it, using JavaScript tests and tools such as Postman.
- Verify via Bank's internal systems (Core Banking System/Data Warehouse) if the new/existing user was properly defined. To ensure the verification of this scenario, alignment meetings with the representatives of the bank will be put in place.

- ○ Verify via Active Directory for Single-Sign-on if the proper user permissions are set for TORP/AD users.
- ○ Ensure the integration of TORP did not affect any functionality of the base product and/or third-party systems.
- ○ Ensure proper warning and error messages are received by the user throughout the flow.
- ○ Verify if an existing user has old data (married, changed name, updated home address) after ID Cardscan and the if data can be updated via Core Banking System.
- ○ Negative tests with fake ids (edited in photoshop and scan the image with fake data) to ensure the system behaves in a proper manner.

Non-Functional tests will focus on performance, usability and security. For performance we will define thresholds for the maximum number of users and tests against these, using JMeter. Usability tests shall be focused on respecting any Brand design and Tremend's internal usability rules. Security tests shall be performed using OWASP Zed Attack proxy and manually verifying the results for any false positives.

If required, additionally to the manual functional tests, Tremend can develop a functional test automation suite that can speed up the verification process and reduce the regression test time. The prioritization of automating test cases shall be done on the set priority from Testrail, focusing on the time-consuming test cases.

You can check a white paper on the methodology in this additional document:

Tremend Methodology - 02. QA.pdf

8.3. Security - Secure Software Development Life Cycle

Tremend employs a Secure Software Development Life Cycle (SSDLC), primarily based on the Software Assurance Maturity Model (SAMM) from the Open Web Application Security Project (OWASP). Tremend has a delegated Security Architect (SA) that works closely with the Project's Technical Leader (PTL) and the development team to apply the SSDLC.

Tremend ensures the Governance business functions of the SSDLC applies at the organizational level, while the Construction, Verification & Deployment functions are adjusted & established in agreement with the client and its representatives, by identifying applicable policies and standards and mandates that the software will need to follow.

Tremend has built a knowledge base of security considerations & best practices as well as recommendations/ approaches for each, and approaches it from an agile perspective, by making sure that:

- Essential security practices are to be performed with each major release;
- CI flows should include automation of security test suite for major releases.

Specific Bank's IT Security and Operational Risk Management requirements will be considered in the analysis phase, along with the non-functional requirements for the platform.

The infrastructure will implement at least the following security measures:

- Web access via HTTPS only;
- Containerized solution components - the only exposed container is the NGINX one for SSL termination;
- Service access only via SSH with public-private key pair authentication;

- Load-balancer with a firewall for access - with the possibility to condition the access based on originating IP;
- Configurable data encryption;
- Full monitoring and logging with 6 months log retention.

You can also check Tremend's Secure Software Development Life Cycle here:

Tremend Methodology - 03. SSDLC.pdf

09. Timeline and Costs

–

9.1. Timeline - Digital Onboarding MVP estimation

Starting from a vanilla version of the Digital Onboarding solution and based on Tremend expertise in similar implementation projects, we estimate 1 Sprint for Discovery phase and 2 Sprints for project implementation time.

	Period	Month 1				Month 2	
		w1	w2	w3	w4	w5	w6
Project phase		Sprint 1		Sprint 2		Sprint 3	
User interface	Design	🟦	🟦				
	Feedback implementation		🟦				
Analysis	Business Analysis	🟦	🟦	🟦	🟦		
	Application architecture	🟦	🟦				
	Data schema		🟦				
Development	Implementations Backend			🟦	🟦	🟦	
	Implementations Frontend				🟦	🟦	
	Environment setup			🟦			
	Test instance deployment			🟦			
Documentation	User manual					🟦	
	Deployment Working Instruction			🟦			
QA	Testing				🟦	🟦	🟦
Production release	Production release						■

9.2. Team structure

The following team composition would fit the right mix of skills and velocity required for the project:

- TORP Technical Architect
- Technical Lead
- TORP Business Analyst
- Project Manager/Scrum Master
- Backend Software Engineer
- FrontEnd Software Engineer
- QA Engineer
- UI/UX Designer

9.3. Costs

9.3.1. Cost Structure

TORP's financial offer depends on the following parameters:

- **Infrastructure Model**:
  - **TORP On-Premise** installation relying on Bank's owned infrastructure and services;
  - **TORP SaaS** (Software as a Service) model, which includes the Cloud subscription fee for the SaaS infrastructure and all required administration and operation services;
- **Main Modules -** Onboarding & Origination functionalities or Onboarding functionality only;
- **Licensed Software Modules -** the selected Functional Entities and additional Building Blocks required for the Onboarding / Origination flows;
- **Licensed Capacity -** the committed number of annual transactions generated for:
  - COM **-** ID Card scan & OCR & Selfie face recognition
  - COM **-** Biometric video identification (eID **-** Video ID High Security)
  - DMM **-** Digital Certificate issuance and Electronic Signature
  - DMM **-** External eArchive integration
  - RFDE **-** AI Scoring
- **Customizations complexity**.

Based on the above mentioned parameters, the cost structure is composed on two main components:

- **TORP instance fee (one time charge) -** representing the costs for TORP Perpetual License Fee, instance set-up, customizations & integration costs;
- **Price per transaction -** representing the all-inclusive transactional fee for the Licensed Capacity. The payment schedule for the Licensed Capacity can be annually, bi-anually or quarterly.

9.3.2. Digital Onboarding & Origination pricing examples

As an example, please find below the pricing structure for TORP's vanilla version, including various combinations of platform functionalities (Onboarding / Onboarding+Origination), platform model (on-Premise / SaaS), and Committed Annual Transactions (25K / 50K).

Pricing scheme for TORP Digital Onboarding module:

TORP Platform Model	TORP instance fee	Licensed Capacity Committed annual **onboardings***	
		25,000	50,000
On-Premise	TBD	TBD	TBD
SaaS	TBD	TBD	TBD

Note:

- One Digital Onboarding transaction includes:
    - 5 prospects (email, phone number, ID Card scan and OCR data);
    - one onboarded customer fully defined, identified using our standard identification unattended module, with 2 onboarding documents electronically signed (advanced digital certificate remotely issued for the customer + Bank's advanced digital certificate).

Pricing scheme for TORP Digital Onboarding & Origination modules:

TORP Platform Model	TORP instance fee	Licensed Capacity Committed annual **disbursements***	
		25,000	50,000
On-Premise	TBD	TBD	TBD
SaaS	TBD	TBD	TBD

Note:

- One Loan Disbursement transaction includes:
    - 15 prospects (email, phone number, ID Card scan and OCR data);
    - 2 onboarded customer fully defined, identified using our eIDAS compliant Video Identification module, supervised by a certified agent supplied by Tremend, with 2 onboarding documents electronically signed per customer (qualified digital certificate remotely issued for the customer);
    - one loan disbursed, 3 documents electronically signed per loan (qualified digital certificate remotely issued for the customer + Bank's qualified digital certificate);
    - all generated & electronically signed documents are transferred to our subcontractor's certified electronic archive.

The prices are expressed in EUR without VAT.

10. Confidentiality

–

Tremend undertakes not to disclose to any third party confidential information which Tremend obtained from the client during their collaboration.

Tremend undertakes and warrants that the information received during or in connection with the rendered services in favour of the client will not be used for their own interests or the interests of any other person.