TrustPortal SaaS

Service Description

April 2025

Table of contents

Section A - Overview

Background

Put simply, customers are demanding better service, across traditional and digital channels

The pace of digital adoption across all sectors is accelerating, and hence the expectations of customers for great service is also increasing. Yet customers also demand the personal touch, and hence organisations still need to provide great service through traditional channels too (phone, branches, shops etc).

Organisations acknowledge they must provide a superb customer experience, and compelling digital and multi-channel presence – but that's far easier said than done…

And the no.1 issue to creating a great customer experience is existing IT systems issue – often the inability to integrate multiple legacy systems

Most sectors however have high-cost traditional channels often combined with poor digital capabilities. Even the biggest organisations deliver a "full service" digital experience for only a subset of their products and services. And they must invest tens of millions of pounds to do it, often with poor ROI.

This document must be used in conjunction with the "**TrustPortal Solution General Terms and Conditions for SaaS Services ('GTC')" (**April 2025 or later**)**", and the "**TP Order Form template (for use with GTC) - Execution version"** (April 2025 or later).

What is TrustPortal - common Use Cases

TrustPortal enables digital, robotics and AI to work together seamlessly and help digitize company's legacy systems and provides a dynamic robot human interface. To do this TrustPortal provides multiple capabilities:

Single, one-channel, solutions

HyperForms

Load up your current PDF form, or design interactively and autogenerate TrustPortal digital form, connected to any RPA tool to access any systems, with real-time validation. Secure, fully theme-able for internal or public website use

HyperMail

GenAI and configurable automation are combined to reduce the time taken to fully automate and action inbound email requests by 80% - but safely, with staff fully in control

HyperAPI / HyperChat / HyperHITL

Enhance any channel through access to ALL systems - even those without API's. Plus augment existing GenAI chatbots or GenAI processes with sophisticated real-time digital UI's/journeys

Enterprise, multi-channel, solutions

HyperService & HyperIoT

Digitize and automate every channel, incl. telephony, IVR, chatbot, website, mobile, SMS, IoT and more. Augment existing environment to improve agent productivity by 50%, plus simple customer self-service

HyperCRM & HyperBPM

Leading CRM or BPM systems still struggle with access to old systems, or the effort to create complex agent journeys. Enhance your existing CRM/BPM to connect to everything, and create complex journeys/UI's at 10% of typical cost

HyperOrg

Multi-agency working is often entirely manual. Allow multiple orgs to collaborate around customers or cases easily, securely, across channels, irrespective of the existing IT complexity

TrustPortal has differing levels of SaaS

As well as providing TrustPortal on-premises, TrustPortal is also provided as a software-as-a-service (SaaS)

The following tables summarises the types of TrustPortal SaaS provided

Appendix A shows an example order form, where some of these elements may be varied in the order:

Component	Proof-of-Concept Proof-of-Value	Pilot	Production
Scope	Evaluation of technology or value, but not used live	Evaluation of value for limited number of users, but with production data	Full production service, core to operations
Environments	1 Environment	1 Environment	3 (Dev, Test, Prod)
Key Exclusions	Standard SLA, no variations allowed Uses *.trustportal.net naming Typically: • No integration to SSO • No integration to Channels (e.g. IVR, Chatbot) • No MiniBots	Standard SLA, no variations allowed Uses *.trustportal.net naming Typically: • No integration to SSO • No integration to Channels (e.g. IVR, Chatbot) No MiniBots	Uses *.trustportal.net naming
Hosting	AWS	AWS	AWS
Countries	Global, by agreement	Global, by agreement	Global
RPA Supported	Any supported RPA, up to agreed max users (e.g. 10 concurrent users)	Any supported RPA, up to agreed users (e.g. 10 concurrent users)	Any supported RPA
RPA Hosting	Additional cost	Additional cost	Not available – typically customer or partners provide this
Term	Minimum 1 month	Minimum 1 month	Minimum 3 years
TrustPortal Licenses	Included	Included	Included
Scope	Fixed	Fixed	Size, SLAs etc. all subject to discussion/contract
Info Security	AES256, PPK encryption in transit and rest + HTTPS in/out of SaaS	AES256, PPK encryption in transit and rest + HTTPS in/out of SaaS	AES256, PPK encryption in transit and rest + HTTPS in/out of SaaS
Patches / Upgrades	Only mandatory patches/upgrades	Only mandatory patches/upgrades	Up to 1 full upgrades per year (across dev, test and prod envs)
Maintenance	No proactive maintenance	No proactive maintenance	Proactive maintenance to maintain performance
IT Integration	Design and IT approval support provided	Design and IT approval support provided	Design and IT approval support provided
Onboarding	Customer creates TP accounts for users, sets up processes/roles via virtual roles	Customer creates TP accounts for users, sets up processes/roles via virtual roles.	Full integration with organisation AD/SSO. Customer setups up processes/roles via virtual roles.
Offboarding	All data securely destroyed	All data securely destroyed	Data extracts by customer can be facilitated as part of contract
Auditing	None	None	Subject to agreement
Backup	Nightly backups, up to 1 days data loss	Nightly backups, up to 1 days data loss	Ongoing backups, no data loss
DR	No DR	No DR	Full DR, with recovery time subject to agreement
Firewalls/Intrusions	Full Firewall (https-only) Limited intrusion detection	Full Firewall (https-only) Limited intrusion detection	Full intrusion detection and reporting
Performance Monitoring	No proactive monitoring	No proactive monitoring	Full proactive monitoring and reporting excesses. E2E

			monitoring including into client estate subject to agreement
Availability SLAs	Best endeavours (environment not setup/priced for full resilience)	Best endeavours (environment not setup/priced for full resilience)	Full SLA management and monitoring, defined escalation and roles, setup as 24x7 service
Data Allowed	Dummy data only	Production data	Production data
Data processing	Not possible – all data encrypted, with no TP access to keys	Not possible – all data encrypted, with no TP access to keys	Not possible – all data encrypted, with no TP access to keys
Liability	No liability for data, service levels	Limited liability for data, no liability for service levels	Capped liability for data and service levels
Pricing models	Monthly Fee	Monthly Fee	Yearly Fee

Section B – SaaS Lifecycle

The following pages describe how the TrustPortal SaaS service is designed, provisioned and operated

Phase 0 - Ordering and invoicing process

Ordering the TrustPortal service, or requesting changes, is done by contacting one of the TrustPortal Commercial team – please contact us via the website www.trustportal.org or email sales@trustportal.org

TrustPortal will provision a full production service typically within 5 working days of provision of PO.

Ceasing the accounts is done via the same route of using the TrustPortal Commercial team

TrustPortal expects payment 7 days from Invoice. Invoicing will be in advance for initial setup charges and for annual service provision.

Phase 1 – Design

Overview

The TrustPortal Production SaaS is based on a single-tenant "AAA"-rated AWS infrastructure – i.e., separated environments for each customer, with the scalability, resilience and security of core enterprise systems.

Appendix B describes the standard services within the TrustPortal SaaS

Phase scope

The following are the key components of the Design phase

- Design and signoff in conjunction with organizations IT / security / networking team
- Creation of TrustPortal single tenant environment to customer's design

Any AWS data centre location can be chosen to host the service

Technical Boundaries

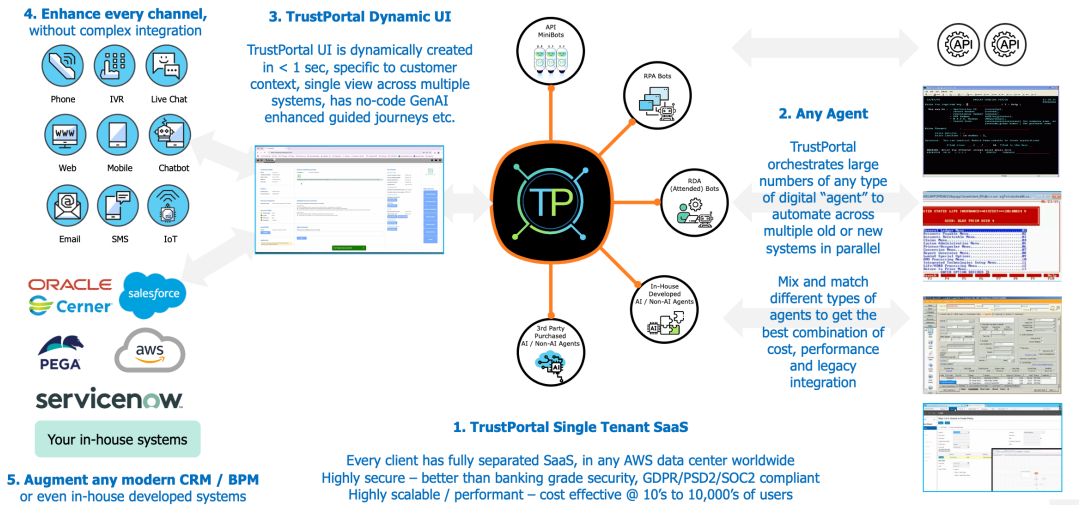
The TrustPortal service, comprising all data stored and the service itself, is entirely hosted in any AWS data centre globally.

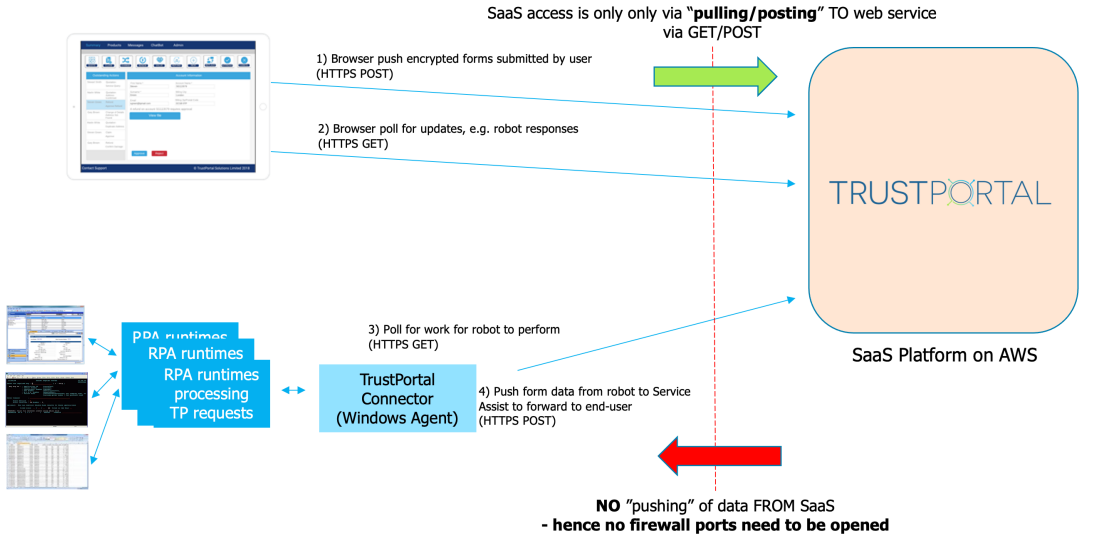
The digital front-end presented to end users is delivered via a secure internet session to end user's browsers/mobile devices. Data is encrypted with AES256 public-private keys (PPK) in the browser before transmission to the TrustPortal SaaS over (further encrypted) HTTPS

The TrustPortal SaaS is then polled for by Robotic Process Automation (RPA) Digital Workers via a TrustPortal Agent that handles the PPK encryption/decryption. Both the digital workers and TrustPortal Agent are typically installed on-premise in the customers data centre – although the TrustPortal SaaS will also work with cloud-based digital workers

The following pictures illustrates the high-level architecture.

8 TRUSTPORTAL SAAS SERVICE DESCRIPTION





Data location

The physical location of the data will be subject to customer choice, and can be located in any AWS data centre globally

Services within AWS are by default setup to span data centres for resilience and DR

Data Centre Tier

All AWS data centres are designed and operate to tier 3

Monitoring

The performance, availability, resilience and security of the TrustPortal service is monitored in real time using AWS tools, and Kibana

In addition, end-to-end monitoring from end user browser to robot and back again can be accommodated via APM, but requires implementation in the customer domain, so is subject to a further setup and operational charge.

Support Boundary

While TrustPortal will endeavour to assist customers with issues resulting from access to the TrustPortal service, limitations of this support may arise because of corporate security controls (e.g. whitelisting, internal approvals).

In this Phase we would also confirm support arrangements (typically based on Appendix C), and training requirements for Customer RPA and Support staff.

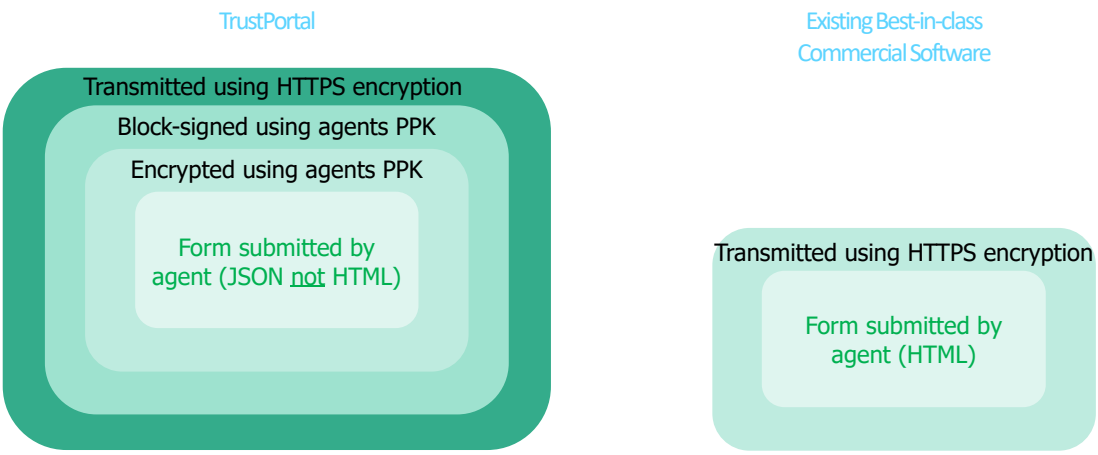
Security

TrustPortal ensures all communications going to and coming from its servers are extremely secure

Firstly, all data going into/out of the TrustPortal SaaS is PPK-encrypted, with separate keys for each user. These keys are not accessible to TrustPortal, and hence all data into the SaaS cannot be read or tampered with.

Furthermore, all data blocks going to/from the TrustPortal SaaS are “signed” in a manner similar to blockchain, such that any changes to the data are automatically detected

All data that is in transit to/from the TrustPortal SaaS is encrypted over HTTPS/TLS 1.2+ connections – effectively TrustPortal data is double encrypted



Typical Attack Type	Security Issue in Typical Application?	Security Issue in TrustPortal?	Why isn't this a problem in TrustPortal?
Poorly formed HTML (incl. SQL Injection)	Yes	No	We don't send HTML data from user browser to TrustPortal
Webserver Architecture (e.g. Apache) vulnerabilities	Yes	No	We don't use a web-server architecture
Credential Sniffing	Yes	No	We use SSO and don't pass unencrypted credentials from browser to TrustPortal
Man-In-Middle Attacks	Yes	No	All data has unique block-signing (like blockchain), any changes corrupt data
API Access Attacks	Yes	No	All data must be correctly encrypted and contents well formed for API to respond
Denial of Service	Yes	No	AWS services intercept/deflect before gets to TrustPortal
Encryption Keys	Yes	No	Separate, auto-generated keys for each user, with keys themselves kept encrypted. Each message has unique AES Key, decrypted using users PPK
Database Access	Yes	No	No direct access to TrustPortal database, all data encrypted with multiple user keys

Integration to Customer Systems

All data going to/from the TrustPortal SaaS goes via defined RESTful API's and is fully encrypted and transmitted over HTTPS – either via an end-user's browser or TrustPortal Agent.

As TrustPortal does not directly connect to client core applications (that is done by RPA robots or other types of agents), there are only a few additional integrations to customer systems:

AD/SSO Integration:
The TrustPortal SaaS can be configured by SAML2 or OpenID, to connect to internal Active Directory and SSO services, such that AD is used for logon authentication

User Role Integration
Where Active Directory does not contain "role" information accessible via SAML2 or OpenID, this can be configured using TrustPortal User Management (TPUM).

Monitoring
The TrustPortal service can be monitored from end-to-end, form browser to robot, using tools such as APM/Kibana or customer enterprise monitoring tools. Basic monitoring is part of the service, but additional E2E monitoring is subject to an additional cost.

Additional Channels
The TrustPortal service can be connected to additional channels such as IVR, chatbots, web sites etc through a RESTful API connecting to a TrustPortal Agent in the customer domain. Further detailed design support for this is subject to an additional cost

AWS Security, Scalability, Resilience and DR

The TrustPortal SaaS uses advanced services within AWS to provide security, scalability, resilience and DR including:

- Route 53 (DNS), Web Application Firewall and Application Load Balancers
- Multiple VM's across availability zones for resilience and DR
- AWS resilient services for MySQL and Redis
- S3 resilient storage
- Cloudwatch monitoring

Add-On TrustPortal Modules

The TrustPortal SaaS includes the running of the standard TrustPortal software

Additional TrustPortal modules may be included in the TrustPortal SaaS, subject to commercial agreement in the TrustPortal SaaS SoW. These may include:

- GenAI Studio - GenAI Designer
- Tasks MiniBot(s)
- API MiniBot(s)
- Enhanced Maintenance and Reporting
- RPA Dynamic Scheduling – coming soon

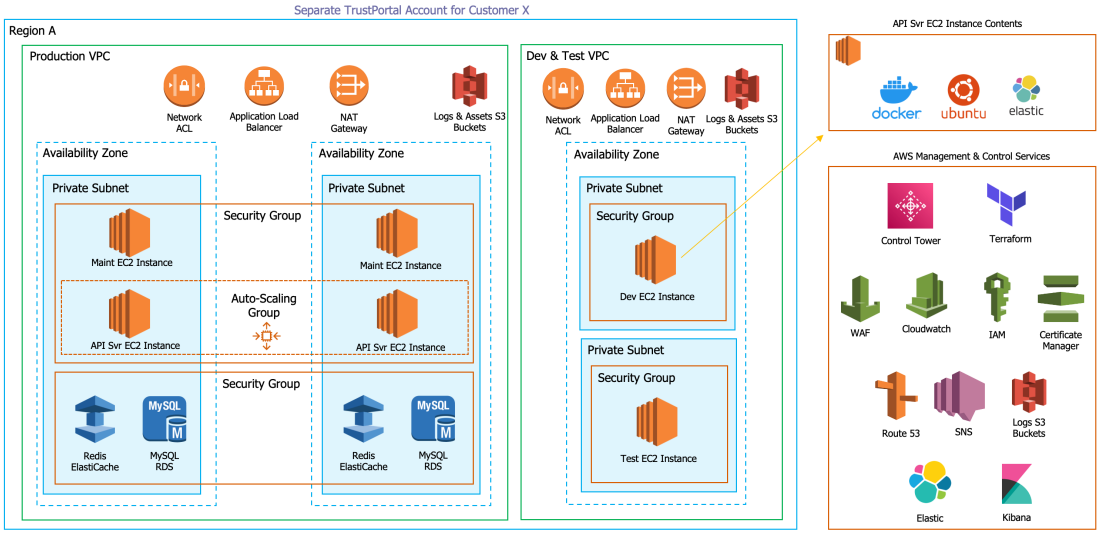
Out of Scope

The following items are out of scope of the TrustPortal SaaS and hence this Phase:

- Design and setup of the RPA environment that connects to the TrustPortal SaaS

Any additional integrations, processes or setup to meet customer specific requirements are out of scope, unless agreed in advance and subject to additional charges

An overview of our typical AWS “AAA”-rated service is shown below



Phase 2 – Customer On-boarding

On-boarding

The summary implementation plan for on-boarding TrustPortal for digital engagement will be part of the statement of work for the TrustPortal SaaS Project.

In most cases the timescales for implementations can be as little as a few days or weeks elapsed time. The precise effort needed will depend on the scope of intent and range of services being connected.

Phase scope

The following are the key components of this phase

- Setup connection to customers RPA or Agentic environment - typically on-premises but may be cloud-based (RPAaaS)
- Confirmation of end-to-end connectivity between components
- Connection to other corporate services (e.g., AD/SSO)
- Setup of users to allow access to TrustPortal SaaS either via AD setup and/or TPUM
- [Optional] Connection to additional Customer channels (e.g., IVR, Websites, Chatbots etc)
- Training for RPA and Support teams

Key Customer Requirements

The following is a list of key requirements to integrate to the TrustPortal SaaS:

- Users having access to internet from their browsers
- Robots having access to the internet from their VM/network
- Whitelisting of the TrustPortal SaaS for end-users and the networks they access internet on
- If robots are on-premise then whitelisting of the TrustPortal SaaS for that network
- Provision of SSL certs
- Modern browsers used by end users (Chrome, Firefox, Edge etc), capable of supporting ECMAScript 2016

To confirm to Customer IT/Security:

- All connection to TrustPortal SaaS is via HTTPS
- All data is additionally protected by AES256 public-private key encryption in transit and rest
- No firewall ports need to be configured on the customer side

Phase 3 – Ongoing Services

Phase scope

The following are the key components of this phase

- Issue diagnosis, bug fix and upgrades and ongoing housekeeping/maintenance
- Availability and performance monitoring, ensuring system up and performing to agreed SLA

Please refer to Appendix B – Description of Services, for a description of the standard services included in the TrustPortal SaaS. This includes:

Security and Information Assurance
Scalability and Resilience
Performance
Backup/Restore
Disaster Recovery
Customer Business Continuity
Maintenance
Patch Application
Upgrades
User and Key Management
VM Security
Infrastructure Baselining and Versions
Access Control and Intrusion Detection
Data Auditing
Service Logging
TrustPortal Configuration Changes
Helpdesk
Channel Connections
Development and Test Environments
Demo / Sandbox Environments
Additional (extra cost) services – e.g. VPN, End to End Monitoring

Data Processing

TrustPortal as a product has a unique, highly secure architecture whereby:

- All data going into the TrustPortal SaaS is AES256 PPK encrypted
- The TrustPortal SaaS does not have access to the PPK keys to decrypt data
- All data going into the TrustPortal SaaS is block-signed (similar to blockchain), for automatic detection of changes

Hence the TrustPortal SaaS cannot read data stored in it or modify it. So, we do not know if data stored is dummy data or production data/personal data/confidential data etc.

Hence while it may be subject to “Data Processing” legislation (e.g. under EU GDPR regulations), for all intents and purposes the TrustPortal SaaS cannot actually “process” data

However, the very high levels of security built into the software and SaaS provides customers with the confidence that TrustPortal complies with GRPR, DPA, PSD2 and other regulatory requirements

Availability Service Levels

AWS's inherent multi-datacentre, fault tolerant cloud based infrastructure result in near 100% operational uptime.

However, in order to support continual enhancement to our service, contractually our service level is 99.8% during scheduled hours

Monitoring of service levels is a standard feature of the TrustPortal SaaS

Support Procedures

The description of Support Levels and the responsibilities are described in the table below:

	Role/Responsibility	Description
1st Level Support	**The Customer** (paying for TrustPortal SaaS)	e.g. end user's queries
2nd level support	**IT Helpdesk of the Customer** (paying for TrustPortal SaaS)	e.g. for service issues
3rd level support	**The Customer** to log a call with the **TrustPortal SaaS support team** via the support portal.	e.g. for service issues, bugs, enhancements

Issues reported through the support portal will be logged within our support tracking system and responded to according to severity and priority. For major incidents including service availability, additional direct telephone hotlines can be provided on request

Support Priorities

The definition of support priorities and standard default times are defined in the table below:

Priority	Definition	*Target Response Times*	*Target Resolution Times*
P1	The entire TrustPortal Software is unavailable resulting in a critical impact on Customer's business	Initial Response 1hr Updates every 1hr	within 4 hr
P2	Operation of the TrustPortal Software is severely impacted having a critical business impact on multiple automations	Initial Response 4 hrs Updates every 4 hr	within 8 hr
P3	Non-critical function or procedure, having some operational impact, but with no direct impact on services availability. Typically a *workaround* is available.	Initial Response 8 hr Updates every 1 business day or as agreed in issue	within 48hr
P4	Low priority issue / minor inconvenience but there are typically *workarounds* or alternates.	Initial Response 48hr Updates every 2 business days or as agreed in issue	as soon as practical

Definitions of the terms relating to Support and Maintenance are described below:

	Definition
Target Response Time	The period of time from receipt of a Support Case during which TrustPortal will use its reasonable endeavors to acknowledge the initial notification of the Support Case, communicate an incident reference number and allocate a priority level
Target Resolution Time	The period of time from the point at which it is confirmed by TrustPortal that a Support Case is due to an Error during which TrustPortal will use its reasonable endeavors to provide a resolution to the *Error*. Any period of time during which TrustPortal is unable to progress the Support Case due to any delay in providing information or collaboration by Customer will be excluded from this time. The target resolution may be the provision of a suitable *Workaround*. Where appropriate TrustPortal will continue to work towards a permanent correction of the *Error* as soon as reasonably practicable, but measurement of the Target Resolution Time will cease at the point at which a *Workaround* has been provided.
Workarounds	A method, action or procedure recommended by TrustPortal which in TrustPortal's reasonable judgment avoids the effects of an *Error*.
Error	A failure of the TrustPortal Software, due to errors in the code, to perform in accordance with its Specification

Channel Connections

RESTful API connection support can be used by channels such as IVR, Websites, Chatbots, Voice Recognition etc and is included in the price of the service and documented on our Wiki.

However, diagnostics around issues with these channels is not supported unless added to the standard service

Phase 4 – Customer Off-boarding

Off-Boarding

We will close your TrustPortal Account with us at the end of the Contract.

We will archive your Data after your Account is closed, and you will not be able to access your Data.

You will be able to retrieve your Data for up to 30 days after the Account is closed. We may charge a fee for this service.

Note however all data stored in TrustPortal is encrypted and we do not have keys to decrypt. So exported data would only be of use if setup into another identical TrustPortal environment

Once the period has been reached, we will delete your Data and it will not be recoverable. We will not be responsible to you for any Data that you are subsequently unable to access or retrieve when your Account closes.

All the infrastructure, VM's, disks, backups etc. will be destroyed at the end of the contract. All disks will be wiped used AWS secure erase procedures

Termination terms

TrustPortal Services are subject to the terms defined as part of the Statement of Work

Part 5 – Customer responsibilities

Concurrent Users and Connection

The customer must ensure that the maximum number of concurrent users and connections is within the procured amount. TrustPortal will alert the customer if this is breached

The definition of concurrent users is in our Wiki at https://trustportalhelp.zendesk.com

End User Devices and Browsers

In general, TrustPortal assumes the following to be responsibilities of the Customer wrt end-user devices and browsers.

The software is accessed through a web browser or RESTful API via the TrustPortal Agent so there are few technical requirements and indeed TrustPortal has implemented it service to be largely browser agnostic.

Software is typically accessed through a web browser for end users – either internal or external

Customer browsers must be able to support ECMAScript 2016, for example:

Microsoft Edge: V97.0.1072.76+
Chrome: V98.0.4758+
Mozilla Firefox: V96.0.3+
Safari: V15.0+

Note: Given the dropping of support by Microsoft, Microsoft IE11 is no longer supported

The software does not place high demands on bandwidth but adequate connectivity to access the software is required.

Also, as data is decrypted in the end users browser, then browsers and devices compatible with hardware decryption are recommended for best performance

Support from Customer Resources

There are a number of areas that the setup and operation of the TrustPortal SaaS is dependent upon access to suitably skilled and empower customer resources/teams.

Examples include (but are not limited to):

- IT and Security teams, for design and signoff of TrustPortal SaaS connection to customer domain
- Network teams for whitelisting of TrustPortal SaaS, diagnosing networking issues
- Active Directory and SSO/SAML2/OpenID teams

- RPA Support teams to assist with the connection of the TrustPortal SaaS to RPA digital workers, and ongoing triage of issues between digital workers and the SaaS
- Channel Support teams to assist with connection of TrustPortal to agreed additional channels e.g. IVR, Websites, Chatbots
- Helpdesk teams to assist in triage of issues, prior to raising issues with TrustPortal SaaS support

Part 6 - Other Services

Training

In all client engagements TrustPortal places a high value on enabling effective knowledge transfer between ourselves and our clients, and can provide appropriate training tailored to client requirements including RPA support team, developers, IT Helpdesk etc.

Digitisation Process Scoping and Build

The TrustPortal SaaS provides a highly configurable digitisation platform working in conjunction with RPA digital workers and AI.

The scoping and building of new processes based on TrustPortal/RPA/AI is out of the scope of the TrustPortal SaaS and provided by TrustPortal partners/resellers.

Please refer to our website (www.trustportal.org) for resellers in your region, or your TrustPortal sales contact

Appendix A – Details of Service

The following describes the scope of the production TrustPortal SaaS that can be provided to customers, and should be included in any SoW

	In Scope?	Bespoke Requirements Possible?	Comments
Single Tenant	Single tenant by default		
Primary Data Centre / Availability Zones	TBC		
DR Data Centre / Availability Zones	TBC		
Hours of Operation	8am – 8pm, Mon-Friday for defined location and with agreed maintenance windows and SLA	Up to 24 x 7 with agreed maintenance windows and SLA is available at extra cost	
SLA	99.8% availability during scheduled hours of operation	Increased availability at additional cost	
P1 Response	Initial Response 1hr Updates every 1hr		
P2 Response	Initial Response 4 hrs Updates every 12 hr		
P3 response	Initial Response 8 hr Updates every 24hr		
P4 response	Initial Response 48hr Updates every 2 days or as agreed in issue		
Maintenance Window	8 hours/month total, @ Sunday nights 8pm UK time		
DR Recovery Time Objective (RTO)	4 hours from customer confirmation to invoke DR		
Upgrades	Max 1 per year with times to be agreed. Upgrades may be needed to keep current with TrustPortal Software End-of-Life (2 years)		

Channel Connections	Standard connections permitted to customer browsers and RPA digital workers	Additional connections to other channels can be agreed (e.g. IVR, websites, chatbots), but may require additional costs	
VPN Setup	No VPN's will be used in creating connection from customer to SaaS	Specific secure VPNs with defined IP ranges can be agreed, subject to additional costs	
DR Testing	Annually, and on each upgrade		
Backup	Full backup at VM level (7 days retained) Full point-in-time recovery up to 30m at database level		
Backup/Recovery Testing	On initial installation, then annually		
Data Encryption in transit	AES256 PPK with individual user keys, over HTTPS		
Data Encryption at rest	AES256 PPK with individual user keys. Encrypted VM images and disks		
Customer AD/SSO Integration	Standard, including TrustPortal User Management (TPUM) integration		
Data Auditing/Export	Not possible – TrustPortal doesn't have keys to encrypted data		
Availability Reporting	Standard AWS Reporting		
Performance Reporting	Standard TrustPortal Reporting	APM-based E2E reporting (including client RPA and users) is available subject to additional costs	
Firewall Setup to support Protocols	HTTPS (Port 443)		
Periodic Penetration Testing	Support for annual customer-initiated pen testing only		
Internal Audits incl. access, risk, regs and controls	Performed annually		
External Audits	Not supported as standard		

Regulatory Reviews	Annually		
Hosting Provider Switching	Not in standard scope	Subject to agreement/additional cost	
Specific network routing	Not in standard scope	Subject to agreement/additional cost	
Infrastructure Documentation	Provided on installation		
Exportable VM images	Not in standard scope		
Other Customer Specific requirements		To be defined here	
Infosec Contacts	See Schedule 5 for key roles that should be defined		
Escalation Contacts	See Schedule 5 for key roles that should be defined		
Issue Reporting	Via TP Portal at https://trustportalhelp.zendesk.com 24 x 7 x 365 Telephone support 0808 1694367		

Appendix B – Description of Services

Security and Information Assurance

In addition to banking-grade "boundary-layer" security, TrustPortal is architected such that all data is encrypted, both in transit and while stationary, with fine grained permissions regarding how companies can see or update customer information.

By default, all TrustPortal SaaS environments are single tenant, and customers choose to host in any AWS data centre globally

Scalability and Resilience

TrustPortal SaaS services are hosted on AWS and utilise the full capabilities of the platform.

Hence TrustPortal SaaS can provide "AAA"-rated security, resilience and performance, equivalent to core internal systems – i.e. TrustPortal can provide the "mission-critical" services in core operations such as contact centres, external websites etc.

Performance

TrustPortal is scaled to provide a highly performant system based upon agreed user/digital worker numbers, with calls to the SaaS being made within 1s for 98% of transactions

Note that customer and internet network issues may impact end-to-end response times, and so are excluded from these times.

Also note the time to render screens on an agents browser, or to receive requests for a digital worker are dependent upon the complexity/size of the data passed, browser performance and hardware/decryption capabilities in the customer estate.

Please contact TrustPortal support or refer to our Wiki for the latest recommended hardware/browsers/sizing guidelines for a given TrustPortal version

Backup/Restore

Backups are fully encrypted and stored at pre-defined AWS datacentre environments (Glacier offered for production).

Backups are at two levels:

- Virtual machines used in provision of services
  This is backed up every night, with backups retained for 7 days

- MySQL Database used to store TrustPortal forms, user information, queue items
  We used an AWS service, with point in time recovery possible up to 30 mins interval

Disaster Recovery

To ensure the TrustPortal operation can withstand and recover from 'disaster' the platform is hosted by AWS in a multi-data centre arrangement

Scenarios in which AWS would implement Disaster Recovery are incidents which affect the availability of the primary data centre as a whole. Examples might include an extended power outage, network outage or a natural disaster.

The likelihood of such outages occurring is minimised as much as possible through resiliency features including Uninterruptible Power Supplies (UPS), on-site generators and multiple independent network providers. DR provision is distinct from the high availability features included in the platform and isn't intended to provide "hot failover" between data centres.

It forms part of the business continuity plan and ensures continued service delivery in the event of a significant business-impacting incident.

Disaster Recovery is provided at the Secondary Datacentre.

An Organisation Virtual Data Centre (OvDC) is created at both Production and DR sites allowing access to both environments. The supported method for DR is database and VM replication of data between Production and DR Cloud environments.

In the event of a DR scenario IP load balancing at the upstream ISP allows the service to be failed over to the DR site automatically.

The typical recovery time objective in case of DR is 4 hours

Customer Business Continuity

Is part of the Phase 1- Design we will support the design of the TrustPortal SaaS to ensure compliance with the customer business continuity plan. This DR capability will be tested as part of the installation

We also test our DR capabilities every year, or after every upgrade, and would look to coordinate this with tests of end-to-end Business Continuity plans – e.g. including RPA DR, core systems etc.

Maintenance

The TrustPortal SaaS service provides pro-active monitoring of key attributes in order to ensure continuity of service and high performance

This includes disk monitoring, database monitoring, log monitoring, key table monitoring etc.

Depending on this monitoring then pro-active maintenance will be performed to ensure service and performance us maintained

Patch Applications

All patching for the TrustPortal SaaS is included as part of the service including:

- TrustPortal software
- Dependent product software (e.g. MySQL, Redis)
- Linux and O/S-Level software

This patching will normally occur in scheduled out of hours downtime, but may be performed in-hours for emergency requirements (e.g. P1 outage)

Upgrades

The TrustPortal SaaS allows for one upgrade per year included in the cost.

This means upgrades across dev, test and production environments, coordinated with the customers RPA team (e.g. to upgrade the TrustPortal Agent) and IT team (e.g. to ensure SSO still working)

Upgrades are scheduled based on agreement with the customer, and do not have to be taken.

Note however the typical lifecycle of TrustPortal versions is that they are supported for two years, and hence if the TrustPortal version becomes unsupported, then upgrade of the TrustPortal SaaS will be mandatory. TrustPortal Support will give at least 90 days notice if a mandatory upgrade is required.

User and Key Management

All key management is automatic within TrustPortal and the team providing the TrustPortal SaaS service **have no access to customer keys**

Public-Private Keys for TrustPortal are stored within TrustPortal in an encrypted form, and can only be decrypted with suitable authentication (e.g. correct TrustPortal password, or SSO authentication)

Hence if users forget their passwords, then the TrustPortal software cannot access any data for that user, and resetting the password will create new keys and all data is deleted.

Hence it is recommended that users are created within TrustPortal with the “share keys with root user” option, in which case the TrustPortal Root/Admin (managed by the Customer) can reset passwords without data loss.

VM Security

TrustPortal uses a number of Virtual Machines (e.g. Auto-scaling Linux VM's) and AWS services (e.g. MySQL, Redis)

All of the Virtual Machines have disks encrypted and only accessible from TrustPortal personnel via secure login. Similarly, all MySQL and Redis services are secured/encrypted by default, and not externally accessible apart from specific defined requirements as part of the TrustPortal service

Infrastructure Baselining and Versions

All components of the TrustPortal service use baselining and version control at the AWS level. Hence all infrastructure components can only be updated by TrustPortal SaaS admins.

In addition, all software on the Virtual Machines is secured both by SELinux (secure Linux preventing unauthorised changes to core files), as well as the use of signed Docker images for TrustPortal software

Access Control and Intrusion Detection

The TrustPortal SaaS makes full use of the AWS Intrusion Detection capability, DDOS prevention etc.

Any unauthorised access will be reported to the Customer team (see Appendix D), as well as Police notifications for DDOS attacks

Data Auditing

As add data stored in TrustPortal is encrypted with keys that TrustPortal has no access to, then data auditing is limited. Also, we have aggressive data retention policies, such that data passing through the TrustPortal SaaS (e.g. going from browser to RPA or back) is deleted as soon as it's been acknowledged as received securely – i.e. no data is stored for longer than is necessary

Hence auditing of data going into and out of TrustPortal is best done by the RPA processes that interact with the TrustPortal SaaS

Service Logging

While the details of data stored in the TrustPortal SaaS is limited (see Data Auditing), then there is extensive logging performed, both at System/Docker level (all the API-level transactions going to/from the TrustPortal SaaS), as well as the database level.

However, for the reasons explained this logging is only of “meta-data” -i.e. “User A send a Form at 11:00:00, and a response came back at 11:00:05”, but not the contents (in this case the form data is encrypted, so not readable)

TrustPortal Configuration Changes

TrustPortal has a built-in Admin Console in the product, that is used by Customer Admin staff to administer the TrustPortal SaaS – e.g. adding users, changing themes, monitoring performance etc.

Where there are additional requirements for managing the TrustPortal configuration that are not possible through the Admin Console, then these requests should be logged though the TrustPortal support portal, and will be addressed typically as Priority 3 items

Helpdesk

There is a support helpdesk for TrustPortal which can be contacted either by:

- 24 x 7 x 365 Telephone support 0808 1694367
- Raise a case on https://trustportalhelp.zendesk.com

Typically, this helpdesk is accessed either by the Customer RPA team or IT Helpdesk teams. Training for these teams is recommended, and would be performed in Phase 2

Appendix C describes the typical support arrangements, which may be varied as part of Phase 1 - Design

Channel Connections

RESTful API connection support can be used by channels such as IVR, Websites, Chatbots, Voice Recognition etc and is included in the price of the service and documented on our Wiki.

Development and Test Environments

Distinct, separate environments for development and testing are part of the TrustPortal SaaS, to support control deployment into the production TrustPortal SaaS

Note however these environments still have the same level of security as production environments, and with key service differences being:

- Development environments, have a limit of up to 20 users. While backed up they are not subject to DR provisions

- Test environments, have a limit of up to 20 users. While backed up they are not subject to DR provisions

Demo / Sandbox Environments

Distinct, separate environments can be ordered at additional cost for demonstration or sandbox uses.

They are setup for short term operation, and so normally have simple backup/recovery and no DR.

Additional (extra cost) services

The following services can also be included into the ongoing TrustPortal SaaS service at additional cost defined in Phase 1 - Design

VPN

Because TrustPortal utilises PPK as well as HTTPS, it is effectively double-encrypted and hence there is often no need for a VPN between the TrustPortal SaaS and the Customers network

However, an AWS VPN service can be procured with defined IP ranges allowed to access the TrustPortal SaaS if required

End to End Monitoring

If required, additional monitoring from end user's browser to robots and back again, can be procured, typically by implementing APM or Kibana

However, as this entails setting up of components/data sources with the Customers environment, typically with unique requirements per Customer, this work typically requires Design and Setup via the TrustPortal Consulting team

It is then operated by the TrustPortal SaaS service, and a visual browser-based UI is provided to the Customer RPA or IT team

Appendix C – Support Roles and Responsibilities

The following describes the high-level role and responsibilities for support and the link between customer support teams and TrustPortal

(C) = Customer Team
(T) = TrustPortal Team

Customer Team	Role	Impact	Service Level
End User (C)	• Access FAQ / training materials to understand usage • Identify issue and raise with user helpdesk	• Explain issue and scale of impact	• Customer response times
User Helpdesk (C)	• Capture incident and determine impact • Resolve end user issue • Escalate as required	• Scale of impact: ○ 1 user impacted ○ Team/site impact ○ All users impacted	• Customer response times
RPA Support (C)	• Triage the issue • Check customer applications are working / check availability reports • Escalate to Level 1 IT Team (Customer) or TrustPortal Support	• Escalate to internal teams and/or TP as required	• Customer response times
Level 1 IT Support (C)	• Capture case on customer service desk system • Review FAQ checklist • Escalate to customer teams or TrustPortal Support	• Log case with TP	• 24 x 7 x 365 Telephone support 0808 1694367 • Raise a case on https://trustportalhelp.zendesk.com
TrustPortal Support (T)	• Triage Issues (RPA / TP / AWS) • Check TrustPortal and AWS configurations • Capture logs • Escalate to teams	• Issue resolution in X hours depending on P1-4 • Escalation for S/W or AWS problems	• Fix within X hours depending on P1-4
TrustPortal Internal Teams (T)	• Triage Issues (RPA / TP / AWS) • Resolve Issue • Configure AWS • Escalate to RPA teams	• System recovery if required • Patch in X hours/days based on priority	• Fix within X hours depending on P1-4 • System recovery within 4 hours

Outside of these support roles and responsibilities for defined incidents, these teams will also be coordinated with for proactive work e.g. upgrades

Appendix D – Governance

The following table describes the typical roles, responsibilities and governance meetings to manage the TrustPortal SaaS, and should be included in any SoW

Role	Contact name	Company	eMail	Meeting Freq (M=Monthly/Q=Quarterly)	Work Phone / Mobile
Customer Business Owner	<Insert here>	Customer	<Insert here>	Q	<Insert here>
Service Manager	<Insert here>	Customer	<Insert here>	Q,M Monthly Chair	<Insert here>
Procurement/ Vendor Manager	<Insert here>	Customer	<Insert here>	Q Quarterly Chair	<Insert here>
Customer Intelligent Automation Team (First Line Support)	<Insert here>	Customer	<Insert here>	M	<Insert here>
Customer IT Support Team (Second Line Support)	<Insert here>	Customer	<Insert here>	M	<Insert here>
Distribution list to be used by TrustPortal when notifying Customer teams of service issues / changes	<Insert emails here>				
Customer nominated contacts to call TrustPortal	<Insert names here>	Customer	<Insert emails here>	Phone	<Insert phone numbers here>
Commercial	<Insert here>	TrustPortal	<Insert here>	Q	<Insert here>
Executive Escalation	Chris Lamberton (CEO)	TrustPortal	chris@trustportal.org	N/A	07711872233
Customer Onboarding	<Insert here>	TrustPortal	<Insert here>	As per project plan	<Insert here>
Support Helpdesk		TrustPortal	Issues logged via Zendesk	M	0808 1694367
Support Escalation	David Linten (CTO)	TrustPortal	David@trustportal.org	M	<Insert here>

Meetings:

- **Monthly Service Review**
    1. Introductions and Personnel Changes
    2. Review of Previous Minutes
    3. SLA Delivery Performance
    4. Issues/Incidents
    5. Invoices
    6. Change
    7. AOB

- **Quarterly Governance Review**
    1. Introductions (New Attendees and Personnel)
    2. Company announcements
    3. SLA Delivery Performance (review and forecast capacity)
    4. Incident management (Supplier issues/3rd party issues)
    5. Financials (current PO/Invoices)
    6. Operational Governance
        1. Contract
        2. BCP
        3. Security/certification
        4. Compliance
        5. DPA breaches
        6. Risk management
    7. Service Improvements (delivered/proposals)
    8. Planned updates/ changes (next 3 months on both sides)
    9. Projects and change requests (new projects and CR)
    10. AOB and next meeting

- **Annual DR Review**
    1. Introductions and Personnel Changes
    2. Review of Previous Minutes
    3. DR and BC planning
    4. DR test review
    5. DR change requests
    6. AOB

Appendix E – Standard Reporting

The following table describes the typical reporting used to manage the TrustPortal SaaS, and should be included in any SoW

Platform	Report	Frequency	Detail	Online/sent
AWS*	Server uptime	Hourly	To be Agreed	Sent
AWS*	Platform uptime	24x7x365	To be Agreed	Online
AWS*	Dashboard reports	24x7x365	To be Agreed	Online
AWS*	Data Usage & Capacity	To be agreed	To be agreed	Online
TrustPortal	TP uptime			TP Admin
TrustPortal	Agent uptime			TP Agent

*AWS - TP to share AWS dashboard (MVP) for go live then discuss with RPA support to adjust reports and errors as platform is used and extended.