**THE AUTHORITY’s SERVICE REQUIREMENTS:**

MULTI FACTOR AUTHENTICATION,

EMAIL AND SMS CAMPAIGNS

AND

MULTI DEVICE MESSAGING

Table of Contents

[DEFINITIONS 4](#_Toc54570267)

[**1.** **INTRODUCTION** 5](#_Toc54570268)

[**2.** **BACKGROUND – THE AUTHORITY** 7](#_Toc54570269)

[**3.** **BACKGROUND – Multi Factor Authentication (MFA)** 7](#_Toc54570270)

[**4.** **BACKGROUND – EMAILS AND SMS CAMPAIGNS** 8](#_Toc54570271)

[**5.** **BACKGROUND – MULTI DEVICE MESSAGING** 8](#_Toc54570272)

[**6.** **TYPES OF SMS CAMPAIGNS AND EMAILS ISSUED** 8](#_Toc54570273)

[**7.** **MFA – CURRENT SCOPE** 10](#_Toc54570274)

[**8.** **EMAIL AND SMS CAMPAIGNS – CURRENT SCOPE** 11](#_Toc54570275)

[**9.** **REQUIREMENTS** 13](#_Toc54570276)

[**10.** **VOLUMES** 17](#_Toc54570277)

[**11.** **DATA SOURCES/DATA CATEGORISATION/REACH** 19](#_Toc54570278)

[**12.** **LANGUAGE** 21](#_Toc54570279)

[**13.** **USER INTERFACE** 21](#_Toc54570280)

[**14.** **TEMPLATES (Day1)** 22](#_Toc54570281)

[**15.** **TEMPLATES (Day 2)** 23](#_Toc54570282)

[**16.** **DESIGN FUNCTIONALITY** 23](#_Toc54570283)

[**17.** **PERSONALISATION** 23](#_Toc54570284)

[**18.** **OTHER FEATURES MUST INCLUDE THE ABILITY TO:** 24](#_Toc54570285)

[**19.** **SECURE EMAIL ADDRESS** 26](#_Toc54570286)

[**20.** **EMAIL ADDRESS DATABASE** 27](#_Toc54570287)

[**21.** **EMAIL DISTRIBUTION** 27](#_Toc54570288)

[**22.** **CUSTOMER PORTAL** 28](#_Toc54570289)

[**23.** **MANAGEMENT INFORMATION (MI) REPORTING and DATA ANALYSIS** 28](#_Toc54570290)

[**24.** **REPORTING** 29](#_Toc54570291)

[**25.** **TRACKING** 33](#_Toc54570292)

[**26.** **TRAINING AND GUIDANCE** 33](#_Toc54570293)

[**27.** **DATA ANALYSIS / PREVENT RISK OF FRAUD** 34](#_Toc54570294)

[**28.** **INFRASTRUCTURE** 34](#_Toc54570295)

[**29.** **INTEGRATION** 36](#_Toc54570296)

[**30.** **INTEGRATION WITH QUADIENT (Day 2 requirement)** 37](#_Toc54570297)

[**31.** **EXISTING ARCHITECTURE** 37](#_Toc54570298)

[**32.** **IDENTITY** 43](#_Toc54570299)

[**33.** **CONNECTIVITY** 44](#_Toc54570300)

[**34.** **CUSTOMER ACCESS** 45](#_Toc54570301)

[**35.** **SECURITY** 45](#_Toc54570302)

[**36.** **SYSTEM ACCESSES AND CONTROLS** 47](#_Toc54570303)

[**37.** **DATA STORAGE** 47](#_Toc54570304)

[**38.** **AUTHENTICATION** 47](#_Toc54570305)

[**39.** **SOFTWARE UPDATES AND SOFTWARE MAINTENANCE** 48](#_Toc54570306)

[**40.** **SERVICE RESILIENCE** 48](#_Toc54570307)

[**41.** **IMPLEMENTATION PLAN/MIGRATION** 49](#_Toc54570308)

[**42.** **SUPPORT SERVICE REQUIREMENTS** 50](#_Toc54570309)

[**43.** **PRIORITY LEVELS** 51](#_Toc54570310)

[**44.** **FAULT RESPONSE** 52](#_Toc54570311)

[**45.** **INVOICING** 52](#_Toc54570312)

[**46.** **SERVICE & CONTRACT MANAGEMENT TEAM** 54](#_Toc54570313)

[**47.** **FUTURE DEVELOPMENT** 55](#_Toc54570314)

[**48.** **APPENDIX 1** 56](#_Toc54570315)

[**49.** **APPENDIX 2** 59](#_Toc54570316)

# DEFINITIONS

In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| "The authority"  “The supplier” | means HM Revenue & Customs, the contracting authority and receiver of the services;  means the person, firm or company with whom The Authority enters into the Contract |

## **INTRODUCTION**

* 1. The Authority is looking to identify a Supplier to take on and transform the existing services including; MFA SMS (OTP) and Voice Calling, outbound email and SMS capabilities (including multi device messaging), currently supported by multiple Suppliers. This new combined email and text service will be a part of a range of Communication Services that will support The Authority’s strategy of communicating with the right customer at the right time through the right channel.
  2. It is critical that the service supports The Authority’s objectives and so, as well as the provision of core functionality and capability Service resilience, the maintenance of Customer confidentiality and building of customer trust will be critically important given that The Authority continues to be one of the most highly phished organisations in the UK.
  3. The successful Supplier must deliver the new service in two phases:
     1. Day 1:
        1. Transition of the existing range of services to one service solution.
        2. Have the capacity to deliver at least eighty (80) million SMS and eight (8) million Voice Calls each year in relation to the Multi Factor Authentication (MFA) service utilised by customers.
        3. Have the capacity deliver at least fourteen (14) million SMS messages associated with Campaigns with the current peak demand requirement of 1.5 million per day.
        4. Have the capacity to deliver at least two hundred and twenty (220) million outbound email messages to customers over 1700 bulletins (separate from EOP used for internal Authority email communication)
        5. Have the capacity to create multiple contract groups (in excess of 25) which contain more than 150 numbers, in each.
        6. It is very likely that our use of the service will fluctuate -perhaps significantly, through the proposed contract life cycle so flexibility of design and charging models will be critical.
     2. Day 2:
        1. We are looking to exploit the top quartile capabilities provided in the solution to develop new and innovative ways of communicating with our customers, whether that be on a 121 or 1 to many basis, in a way that work seamlessly and through standard interfaces where necessary with The Authority’s other Communication and Communication management services.
        2. We are seeking to explore the capability for customers to respond to our SMS campaign messages, for the Supplier to set out how the Supplier would respond to that challenge and provide a cost.
  4. In addition, the service will have to be;
     1. Safe – Customer confidentiality remains The Authority’s number one priority in the delivery of services.
     2. Trusted – The Authority is a prime target for criminal phishing activity. It is vital that The Authority’s customers are able to trust the emails and SMS’s it issues through this service.
     3. Flexible– The Authority seeks to encourage customers to use its increasingly rich range of digital services. Email and SMS, as well as communication channels will be a key enabler of this objective.
     4. Value For Money (VFM) – The Authority believes that VFM is best achieved by being almost totally able to be run and configured by The Authority’s own people. The Authority is also looking for an innovative pricing solution that ensures VFM.
     5. Innovative – The Authority is looking to work with a partner who is imaginative and experienced in the use of voice, email and SMS channels to achieve our Departmental objectives as well as support the day-to-day business of assessing and collecting tax.

## **BACKGROUND – THE AUTHORITY**

* 1. The Authority is the UK’s tax, payments and customs authority, and we have a vital purpose: we collect the money that pays for the UK’s public services and help families and individuals with targeted financial support.
  2. We have three strategic objectives, and everything we do is focused on delivering these for the UK. They are to:
     1. Maximise revenues due and bear down on avoidance and evasion;
     2. Transform tax and payments for our customers; and
     3. Design and deliver a professional, efficient and engaged organisation.
  3. The Authority are designing new systems, products and processes around customers to make it as easy as possible for them to deal with us. Our aim is to become the world’s most digitally-advanced tax authority and we've taken great strides towards achieving this ambition.
  4. The expectations of our customers to be able to manage their affairs digitally is growing and The Authority has invested in new online services which are being used by millions, such as Personal and Business Tax Accounts and online tax credits renewal. Email and SMS services will be critical enablers of the journey to online services and the use of digital accounts.
  5. Effective communication with our customers is a critical enabler and the new Email and SMS services working alongside and integrated with The Authority’s other communication services will play a key role through the life time of the new contract in the delivery of those objectives.
  6. The Authority subcontracts work to its wholly owned company Revenue & Customs Digital Technology Services Limited (RCDTS) and for the purposes of this agreement, services may be consumed or ordered by any authorised employee of RCDTS.

## **BACKGROUND – Multi Factor Authentication (MFA)**

* 1. MFA is used to authenticate individuals or organisations contacting The Authority to enquire about their tax matters.
  2. The Authority manages on behalf of the Government “the Government Gateway”. For those customers who choose to use these services then MFA is used to access the specific services accessed through the Gateway. All individual customers of the Government Gateway (not agents or businesses) must have an MFA SMS verification to allow the customer to proceed no matter which Government Gateway service they use. This could be any service – Tax Credits, Personal Tax Account etc. Some Agents and Business customers must use MFA (Self-Assessment, PAYE etc.), but this is not currently mandated for everyone.

* 1. From Day 1, MFA must be provided in the following formats:
     1. SMS – to any mobile worldwide.
     2. Voice Calling – to any landline and mobile worldwide.
  2. This contract will allow The Authority to provide a managed service type arrangement for other Government bodies (“OGDs”) which allows The Authority to send out MFA (SMSs) on their behalf. The Authority currently has 13 other government services using this capability and this expected to increase over the coming months/years.
  3. Under this managed service arrangement, The Authority will remain responsible for all payments to The Supplier.

## **BACKGROUND – EMAILS AND SMS CAMPAIGNS**

* 1. The Authority currently issues email and SMS campaigns to customers from separate aggregators.

## **BACKGROUND – MULTI DEVICE MESSAGING**

* 1. The Authority currently issues text alerts for HPI/MI’s to senior Authority stakeholders.

## **TYPES OF SMS CAMPAIGNS AND EMAILS ISSUED**

* 1. Help and Support
     1. The Authority issues emails and SMS to customers to provide help and support, to increase upstream compliance and assist customers with understanding their obligations to pay the right tax at the right time or claim the correct benefits at the right time, by providing guidance and/or signposting to digital support products such as webinars, online guides, and The Authority’s You Tube channel.
     2. Examples include:
        1. c. 34 million Help and support emails sent between March and August 2020 for the Coronavirus Job Retention Scheme containing information about the scheme, including from announcements made by the Chancellor of the Exchequer;
        2. Help and support emails sent for the Eat Out to Help Out campaign. 33,000 registered businesses were contacted on separate occasions to:
        3. Encourage them to register for the scheme;
        4. Thank them for registering for the scheme and advise of next steps; and
        5. Signpost them to sources of support, including webinars and You Tube videos.
     3. Approximately 1.3 million SMS sent annually every May to advise customers of increased rates of National Minimum Wage effective from 1 April.
  2. Nudges and Prompts
     1. Nudge/prompt/remind customers to act, either to self-serve or contact us if they need help – either digitally or by telephone. Examples of this include:
        1. The annual Self-Assessment (SA) campaign, where 4 rounds of tailored, targeted Email and SMS reminders are issued every year to approximately 5.2 million customers. The aim is to smooth customer demand in the run-up to the Self-Assessment deadline on 31 January, by encouraging customers to act early and contact The Authority early if they need to do so. Analysis shows to expect up to 5% increase in customer contact rates following sending;
        2. The annual Tax Credits campaign, where in 19/20, 2.3 million SMS were sent to customers to remind them to complete their tax credits renewal form or contact The Authority if they needed help to do this. SMS were sent in carefully timed and staggered batches, so as to manage potential demand.
  3. Provide reassurance and prevent progress chasing
     1. An SMS being sent upon receipt of a form submitted by the customer, to advise it has been received and indicate expected timeframes for next contact. Current volumes are approximately 2,000 per month, with potential to increase.
  4. Seek customer feedback to help improve our services
     1. Between 160,000 to 300,000 SMS are sent every month to customers who have contacted The Authority’s helplines, with a hyperlink inviting them to complete an online survey to provide feedback on their telephone call experience.
  5. Email campaigns and SMS campaigns functionality will never be used to inform customers of a repayment or to ask for payment as part of Customer Service Campaigns.

## **MFA – CURRENT SCOPE**

* 1. The current scope for the MFA Service is:
     1. To send a unique six (6) digit access code to a customer. The Authority will be responsible for the creation and duration of the validity of any access code e.g. 15 minutes.;
     2. The code must be sent to a landline or mobile via SMS (“transactional route”) or Voice;
     3. The user could be in the UK or abroad (anywhere in the world);
     4. The SMS is sent using a single unique short code / unique Sender ID associated with The Authority – this must be provided by the Supplier;
     5. New short codes / Sender ID (registered worldwide) may be required and the Supplier must provide any such numbers at cost;
     6. The voice call must use a unique Calling Line Identification (“CLI”) associated with The Authority – this must be provided by the Supplier;
     7. New CLI numbers may be required and the Supplier must provide any such numbers at cost;
     8. If the customer wishes to call the CLI used for the voice call, this will result in an automated message being played to the customer that The Authority specifies. This call will be free to the customer and The Authority will be charged for this. This must be a 03 (local rate) number; and
     9. Customers must be able to repeat the voice call (i.e. press 1 to repeat), but The Authority must be able to control/configure how many times they can repeat the voice message (currently this is a maximum of two (2) repeats).
  2. The Supplier must be able to:
     1. Block (for both SMS and Voice) specific numbers, ranges/blocks of numbers, countries, networks (including Mobile Virtual Network Operators) at The Authority’s request within two (2) hours, twenty-four (24) hours a day at no additional cost;
     2. Put restrictions/filters on the requests The Authority sends at no additional cost and within two (2) hours; and
     3. Restrict the number of Voice Calls the same number outside the UK can receive in a twenty-four (24)-hour period to a configurable number, currently this is a maximum of five (5), regardless of how many requests are made – this could be to both UK and non-UK traffic.

## **EMAIL AND SMS CAMPAIGNS – CURRENT SCOPE**

* 1. Email campaigns
     1. Emails are currently sent from the secure email address [no.reply@advice.hmrc.gov.uk](mailto:no.reply@advice.hmrc.gov.uk).
     2. Email servers are programmed so that all inbound gov.uk emails are TLS encrypted, this is to ensure courtesy copies and test copies are allowed into The Authority’s email network.
     3. DMARC/DKIM/SPF is also applied as additional security control.  
        With logs sent through to Splunk SIEM for analysis.
     4. Use of hyperlinks in emails
        1. Hyperlinks are regularly used in emails.
        2. Standard header and footer templates contain ‘social’ icons containing hyperlinks to sites of interest to customers, e.g. GOV.UK.
        3. An SSL certificate is purchased by The Authority for a one (1) year period In line with industry standards to allow the use of hyperlinks in emails.
        4. All characters after the tracking domain in the hyperlink are encrypted
     5. Use of macros
        1. Macros are regularly used in emails, especially to personalize the salutation e.g. Dear (customer name).
     6. Email Address Suppression/Bounceback Management
        1. Email Address Suppression is a mechanism that protects the reputation of The Authority’s email domains and ensures messages are not delivered to known problematic addresses and thus affect The Authority’s ability to keep sending messages.
        2. Email addresses are screened against the suppression list and undeliverable emails are not attempted. This reduces costs and safeguards The Authority’s email reputation. Suppressions can be managed through a management interface.
        3. Email addresses that are undeliverable need to be reported. Digital services send single emails and need to report on deliverability of each message.
  2. SMS campaigns
     1. SMS campaigns are currently sent from a dedicated short code, this will be different to the code used by the MFA service (see 7.1 above).
     2. Multiple different SMS campaigns are frequently sent simultaneously.
     3. In compliance with UK Law, no SMS are sent between the hours of 9pm and 8am (GMT) inclusive for this service. For the avoidance of doubt the MFA service (see 7.1 above) SMS and the multi device alert SMS are to be sent 24/7.
     4. Use of robotics and APIs:
        1. Currently there is one SMS campaign that is automated via API and robotics.
     5. Use of hyperlinks:
        1. There is one campaign where a hyperlink is contained in the body of the SMS. Tracking on the number of clicks on the links is available and is reportable.
     6. Use of dynamic content:
        1. Trials have been done previously and successfully to include dynamic field content; however no current SMS campaigns contain dynamic field content.
     7. Home Locator Response facility:
        1. A Home Locator Response (HLR) check is performed as standard on the majority of SMS campaigns. The purpose of the HLR is to check if a number is live or dead before SMS is sent. The exceptions to this are when the data is known to have come recently from the customer. This is at a significantly lower cost than the sending of an SMS. If the check fails, this does not prevent the SMS from being sent. Currently this is set as a 2 hour time window. Dead numbers are then screened against for future campaigns and removed as necessary. This is at nil cost, thus reducing the need to perform and pay for a further HLR (Home Locator Response) check on these numbers. Reporting is available on this in line with SMS reporting requirements.

## **REQUIREMENTS**

* 1. The platform must:
     1. Be a single hosted platform;
     2. An enterprise grade technical platform;
     3. Provide always-on availability with hot failover of key components;
     4. Provide an open and adaptive integration layer supporting all common data transfer protocols (including but not limited to Secure File Transfer (SFTP/SSH), FTPS/HTTPS, Representational state transfer (REST) etc.) For the avoidance of doubt FTPS is The Authority’s preferred method;
     5. De-risk exposure and reduce time to value through with fewer partner solution components and more ‘native’ solutions across the platform supply chain;
     6. Demonstrate and ensure operational agility through streamlined end to end process (less fragmentation/handovers);
     7. Be in receipt of continuous platform investment/updates;
     8. Provide a design and orchestration layer to allow easy creation and maintenance of communications journeys, allowing automated and manual A/B testing when appropriate;
     9. Provide The Authority with the tools and capabilities that demonstrate how emails will render on target email clients, webmail clients and apps (responsive capabilities) in advance of sending them to The Authorities customers (testing);
     10. Be visually configurable (canvas based) and maintainable administratively without requiring deep technical expertise;
     11. Provide a data mastering layer to allow easy and constant cleansing of customer data (The Authorities preference would be for Artificial Intelligence (AI) / Machine Learning (ML) technologies to deliver this requirement);
     12. Allow The Authority to establish and maintain a customer record across all relevant customer data sources to ensure quality of communications journeys with full cross referencing and audit;
     13. Provide a portal capability, capable of capturing communication preferences with integrated content management;
     14. Have a proven scalability track record with linear and elastic scaling;
     15. Provide the capability for a native cross solution analytical function to allow outcome-based measurement of communication strategies, campaigns and journeys, linking with email analytics;
     16. Allow The Authority to scale to more engagement rich digital channels vs lower engagement printed communications and provide broader service options;
     17. Allow the creation of modular content, leveraging a design system or similar solution;
     18. Allow the creation of accessible content, to a minimum of WCAG 2.1 AA;
     19. Be able to send out communications in both English and Welsh languages;
     20. Allow email messages to be sent from multiple domains (e.g. hmrc.gov.uk, tax.service.gov.uk);
     21. Allow SMS multiple user logins for the alert system and ensure there is an audit trail on who has issued the alert;
     22. Allow the creation of name/header/from for each alert issued;
     23. Allow nominated users of the alert system to create/edit/delete:
         1. multiple contact groups; and
         2. templates.
     24. For the text alert system:
         1. interface with The Authority’s ITSM ServiceNow toolset;
         2. allow import of contacts via .csv file; and
         3. confirm who received / read issues SMS or equivalent.
  2. The Supplier must:
     1. Provide a communication platform that can deliver triggered & time sensitive communications (MFA) in a secure and robust method in the appropriate format in a real time or scheduled/pre-planned intervals;
     2. Provide the capability for The Authority to consolidate their existing digital outbound messages (SMS/Email/Push) incorporating journey management that can be edited easily, automating next best actions based on data analysis and customer behaviors, removing or making redundant manual processes;
     3. Allow for omnichannel communications including (but not restricted to) SMS (single and bi-directional), Rich Content SMS (RCS), Email (plain text and responsive HTML), PushIO (for integration of communications into mobile apps);
     4. Allow communications strategies to be incorporated into campaigns and those campaigns to be incorporated into multichannel journeys;
     5. Allow Send-Time optimisation to ensure engagement;
     6. Allow profile-based content inclusion to ensure relevance;
     7. Allow real-time journey switching based on explicit (e.g. change of circumstance) or implicit (observed behaviour / response e.g. opening an email, selecting a link, selecting a button);
     8. Allow sender and subject line prediction/optimisation approaches;
     9. Allow for Artificial Intelligence / Machine Learning (AI/ML) approaches to reduce testing time cycles;
     10. Enable continuous optimisation of communications, campaigns and journeys to ensure best engagement and outcomes;
     11. Allow for the phasing / batching of outbound communications to ensure optimum delivery outcomes;
     12. Provide the ability to set up a dispatch profile for a campaign to allow the user to dispatch x number comms on specific or subsequent days;
     13. Provide a management interface to support this functionality to accommodate short notice changes in the phasing/batching plan;
     14. Provide reporting of suppressions, undelivered messages and bouncebacks to allow transactional services to optimise user communications;
     15. Provide mailbox detection services, including disposable mailbox detection, mailbox verification and group/role-based email checking (to distinguish between individual and organisations);
     16. Allow lists of domains to ensure optimal deliverability of The Authority’s emails; and
     17. Provide the ability to differentiate between statutory and non-statutory notifications.
     18. Provide a platform that is capable of supporting innovation – allowing The Authority to take advantage of new ways of working / communication techniques or tools ‘at pace’.
     19. Respond to The Authority’s change requests within 15 days or sooner;
  3. The solution must:
     1. Allow The Authority to meet both immediate (DAY 1) requirements but allow business driven expansion towards an innovative engagement/journey-based approach in Day 2 without needing to migrate to additional or alternative technologies;
     2. Allow granular and configurable preference management and permissioning (and re-permissioning) via a single-entry point (a portal) as well as via integration APIs;
     3. Allow The Authority to configure their own strategies, campaigns and journeys without need for hands-on technical support;
     4. Provide both operational and strategic analytics;
     5. Provide a native cross solution analytical function to allow outcome-based measurement of communication strategies, campaigns and journeys to ensure maximum engagement;
     6. Provide email analytics function combining Google Analytics with email service provider (ESP) tracking and Litmus tracking to fully inform email design and development strategy; and
     7. Provide optimised data for every step of the marketing journey - right audience, channel, time, content, frequency.
     8. Enable adaptive outreach - leveraging adaptive orchestration as opposed to linear journeys to build individualised experiences and journeys which are executed at scale;
     9. Allow The Authority to create:
        1. one Customer Experience.
        2. flexible Customer Journey Management.
        3. flexible Content Creation & Management.
        4. data as a strategic asset.
     10. Allow The Authority to look to extend the platform’s capabilities to be utilised by The Authority’s call handler Agents, enabling the ability for Agents to issues Emails/SMS to customers on a 1-2-1 basis. Taking into account audit requirements, templates and/or mechanism for messages to be approved before sending.

## **VOLUMES**

* 1. MFA Volumes
     1. The Authority has historically sent over eighty (80) million SMS and eight (8) million Voice Calls each year, this includes a Self-Assessment Peak of over eleven (11) million SMS in one (1) month, January. In addition, the COVID-19 pandemic activities created a peak of fifteen (15) million SMS and six hundred and fifty thousand (650,000) Voice Calls in one (1) month.
  2. The Supplier must:
     1. Have the capability to send as many SMS or Voice Calls that are requested (see volumes at 10.1.1) without any limitations on volumes and at no additional charge to The Authority, other than the agreed unit charges.
     2. Ensure that should volumes reduce, The Authority does not incur any additional charges, other than the agreed unit charge per SMS or Voice Call.
  3. Email campaign volumes
     1. In 2018/19 financial year, 1738 email bulletins were issued to customers, totalling 167.7 million emails with a 98.1% delivery rate, an above-industry standard 29% open rate and a 1.5% click rate.
     2. In 19/20 financial year, 799 email bulletins were issued to customers, totalling 220 million emails, with a 96.66% delivery rate, an again above-industry standard average 28.61% open rate and 1.99% click rate.
     3. Between April to July 2020, the impact of COVID-19 increased volumes, and customer engagement, substantially. 305 email bulletins were issued, totalling 96 million emails, with a 38.14% open rate and 3.34% click rate.
  4. SMS campaign volumes
     1. In 2018/19 financial year, The Authority issued 14 million campaign SMS to customers. These can be categorized into 6 broad campaign areas, with 23 individual sub-campaigns. This includes a Self-Assessment Peak in January each year of over 2 million SMS sent over 2 days on at least 2 occasions.
     2. In addition, 11 million Home Locator Response (HLR) checks were performed during 19/20, to identify dead numbers and remove these from the campaign prior to sending.

## **DATA SOURCES/DATA CATEGORISATION/REACH**

* 1. Email campaigns (currently)
     1. Maximum number of email addresses sent to from one email bulletin is c.5 million.
     2. Over 8 million customer email addresses are held on the email delivery platform.
     3. 411 topic lists, 17 of which are ‘listed’ (visible to the customer).
     4. 22 Categories.
     5. Data has historically been sourced from The Authority’s systems, manually extracted and uploaded to the email platform.
     6. Customers can self-subscribe via online portal.
     7. Customers can ‘self-serve’ to manage their email preferences or unsubscribe from certain, but not all, communications.
  2. SMS campaigns (currently)
     1. Current maximum number of telephone numbers sent to from one SMS campaign is c.2 million.
     2. No telephone number data is currently held on the SMS platform.
     3. Data is source from The Authority systems, manually extracted.
     4. Data is uploaded per SMS campaign.
     5. 25 sub accounts are in place from which to send individual business area SMS campaigns, linked to a central master account.
     6. No opt-out facility (STOP functionality not implemented).
  3. Email and SMS campaigns (Day 1 Requirement)
     1. New data to continue to be manually uploaded/deleted as required via the shared portal.
     2. New topic lists and categories can be created/deleted as required via the shared portal.
     3. Current levels of reach to be accommodated.
     4. Manage preferences and unsubscribe features for customers to self-serve.
     5. For SMS: There is not a requirement to replicate the sub-account structure, but individual campaigns must be individually identifiable and reportable from within the platform.
  4. Email and SMS campaigns (Day 2 requirement):
     1. To work with the Supplier to enable a more integrated solution where data sources feed into the platform and data is fed back to source.
     2. To accommodate future increases to reach as we obtain more email addresses and phone numbers for customers.
     3. To have the ability for customers to choose to opt out of communications they are not obliged to received (i.e. communications more likely to be perceived as marketing) but not be able to opt out of certain communications the Authority is obliged to send where:
        1. The Authority needs to comply with a legal obligation;
        2. It’s necessary for the performance of a task carried out in the public interest or in the exercise of our official authority as a government department
        3. It’s necessary for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

## **LANGUAGE**

* 1. The platform must be capable of sending both voice messages, emails and SMS in both English and Welsh.

## **USER INTERFACE**

* 1. The Authority requires:
     1. An industry leading, interactive user interface to be used by The Authority’s employees to schedule email and/or SMS campaigns, both at the current time and up to a minimum of 1 calendar month in advance;
     2. The capability to amend/cancel an issue up to the scheduled time of issue and select specific dates/times for issue, over extended periods if necessary, e.g. between 10am and 3pm, and provide reporting on this in line with reporting requirements;
     3. The ability for more than one user to be able to schedule email/SMS campaigns simultaneously, and from the same sub-account (if a sub-account structure is applied);
     4. To undertake UAT and adhere to WCAG standards
     5. The solution must have:
        1. User interfaces that are easy and familiar to use and are compliant with HTML 5 UI standards;
        2. device agnostic UI support (Desktop, Tablet, Laptop, Notebook, Mobile);
        3. UI compatibility with all standard Authority browsers (Chrome /Edge/Mobile Safari) and should not require the install of plugins; and
        4. Compliance with current accessibility standards including WCAG 2.1AA.
  2. For email creation:
     1. As a minimum, Industry standard HTML5 and above with CSS capabilities; and
     2. A simple ‘content creator’ interface, giving an ‘easy to use’, ‘drag and drop’ style functionality to build email content and easily undo any changes made whilst at draft stage.
  3. For SMS campaigns creation:
     1. A simple interface to enter SMS characters and any dynamic /personalised content, hyperlinks.

## **TEMPLATES (Day1)**

* 1. For both email and SMS campaigns the ability to:
     1. Easily create new, amend and manage unlimited pre-definable stock templates.
     2. Content Manager: all published templates should be under source control with the ability to roll back to previous versions and provide version history;
     3. Global Resource Handling:  Provide central repository where global CSS styles and resources such as logos/images can be content managed and used for designing templates.  Allow global control over common resources and styles;
     4. Conditional Formatting/Rules (Design Functionality): tools to design targeted comms through variable objects such as text, hyperlinks or images based on data variables; and
     5. Approval Cycle: provide governance for newly created content or templates.
  2. Specifically, for email the ability to:
     1. use ‘email responsive templates’ i.e. responds to the device it is viewed on, e.g. mobile, desktop etc;
     2. create email templates to include changeable banners/images, e.g. the standard ‘Agent’ banner is changed to Agent Updates when we need to use it; and
     3. copy existing draft and sent emails for reuse.
  3. Specifically, for SMS campaigns the ability to:
     1. See how many SMS characters has been used when creating a message.

## **TEMPLATES (Day 2)**

* 1. APIs to allow the upload of templates into the system.

## **DESIGN FUNCTIONALITY**

* 1. Email
     1. The ability to include images and signature images; and
     2. Full text edit functions, placement of text, text size, banners, the ability to format text, headings.
  2. SMS campaigns
     1. The ability to know the number of characters that has been used in an SMS message.

## **PERSONALISATION**

* 1. For both email and SMS campaigns, the ability to support macros/dynamic content to include personalised content, including but not limited to:
     1. Customer names;
     2. Business names;
     3. Reference numbers;
     4. Topic unsubscribes; and
     5. ‘One-click’ unsubscribes.
  2. If none of the above-named fields are available to The Authority, to use a default entry agreed with The Authority.

## **OTHER FEATURES MUST INCLUDE THE ABILITY TO:**

* 1. Insert hyperlinks to GOV.UK and elsewhere, webinar platform, mailbox addresses etc, that need to be hosted in a secure way.
  2. Access Reports, including pre prepared reports in real time and to commission further regular and or one reports as required. As outlined in Section 24 - Reporting.
  3. Set up email/SMS drip campaigns.
  4. Complete A/B testing functionality.
  5. Conduct searches to show all emails/SMS a customer has received, by entering email address and/or telephone number.
  6. Send test emails and/or SMS to users before sending the campaign (e.g. to check if a campaign has been set up correctly, the message looks correctly formatted etc.).
  7. Send a series of test runs and report on these before the campaign is sent.
  8. Include pre-send campaign summary of volumes, wording, cost for SMS (similar to a summary message on your banking app before you transfer money to a recipient). This is to enable The Authority to check expected volumes and costs before sending. Longer term it is expected this requirement will become redundant as the solution is automated.
  9. Receive courtesy copies of all emails/SMS issued once sent.
  10. Use hyperlinks in emails.
  11. Have SSL certificate included in the package, or purchased via the Supplier as necessary.
  12. Have standard header and footer templates containing ‘social’ icons containing hyperlinks to sites of interest to customers, e.g. GOV.UK.
  13. Have encryption on all characters after the tracking domain in the hyperlink.
  14. Use macrosin emails, especially to personalize the salutation e.g. Dear (customer name).
  15. ‘Share’ email bulletins using standard share features and apps, for example, via Facebook, Twitter, Gmail.
  16. Send SMS campaignsfrom a dedicated short code for campaigns.
  17. Sent multiple different SMS campaigns simultaneously.
  18. In compliance with UK Law, no SMS to be sent between the hours of 9pm and 8am (GMT) inclusive as part of The Authority’s campaign service. For the avoidance of doubt the MFA service (see 7.1 above) SMS are to be sent 24/7.
  19. Use robotics and APIs to send SMS.
  20. Interlink SMS campaigns (current and future) operated via robotics with an API to send the SMS.
  21. Use hyperlinks in SMS – SMS to contain the hyperlink in the body of the SMS. Track on the number of clicks on the links is available and be reportable (also mentioned in Section 24 - Reporting).
  22. Use dynamic content to include dynamic field content in SMS (no existing campaigns to migrate but needed from Day 1).
  23. Have a Home Locator Response facility, that users can opt to beperformed as required on SMS campaigns, both before SMS is sent and on datasets where no campaign is scheduled. This is to be at a significantly lower cost than the sending of an SMS. If the check fails, this does not prevent the SMS from being sent, with a 2-hour time window to keep trying the HLR before the campaign is sent by default. Screen for identified dead numbers and remove these from campaigns. Day 1 required is for these numbers to be added to a list to be automatically screened against and removed from future campaigns. This is to be at nil cost, thus reducing the need to perform and pay for a further HLR (Home Locator Response) check on these numbers. Reporting to be available on this in line with SMS reporting requirements (see Section 24 – Reporting). Day 2 requirement is for identified dead numbers to be fed back into The Authority’s systems so they can be removed at source.
  24. The Authority would consider more cost-effective ways of completing this check.

## **SECURE EMAIL ADDRESS**

* 1. The Authority’s email address must:
     1. Be definable ‘from’ address to issue emails and must be ‘no reply’/have no reply functionality i.e. The Authority’s help and support [no.reply@advice.hmrc.gov.uk](mailto:no.reply@advice.hmrc.gov.uk);
     2. Have the ability for the display name and email address to be amended and additional display names and or email addresses to be added;
     3. Allow email servers to be programmed so that all inbound gov.uk emails are TLS encrypted, this is to ensure courtesy copies and test copies are allowed into The Authority’s email network;
     4. Courtesy copies and test copies to be programmed so they can pass through The Authority’s system filters, security and spam prevention shields etc. and are allowed into The Authority’s email network;
     5. Support multiple domains and multiple from addresses to support different channels (Digital Service emails vs The Authority’s ‘Marketing’ emails); and
     6. If a new domain is being used and it is sending as The Authority then there is the need to add the domain to The Authority’s SPF record, then the domain would need adding to The Authority’s O365 TLS configuration and then potentially the domain would need to be added to the “allow list” to prevent it being blocked.

## **EMAIL ADDRESS DATABASE**

* 1. From Day 1 the Supplier must:
     1. Securely store and hold email addresses in specific distribution (topic) lists and those lists to be stored within named categories – topics/categories;
     2. Manipulate email addresses i.e. add, delete and insert into topics in a user-friendly manner;
     3. Be able to import/upload email addresses, up to 5 million;
     4. Be able to migrate existing email address database into new platform and be able to use from Day 1.
  2. From Day 2 the Supplier must:
     1. Work with The Authority to both innovate and automate the email address database, linking in with The Authority’s systems, customer preference tools and automatically identifying and responding to trends in customer behaviour.

## **EMAIL DISTRIBUTION**

* 1. From Day 1 the Supplier must:
     1. Have the capability to allow The Authority to control distribution, ensuring appropriate levels of customer contact with preferably unlimited ‘send criteria’ using logic statements (or similar) e.g. to send emails to customer groups, but exclude all those who may have received previous emails within that day and/or distribution list.
  2. From Day 2 the Supplier must:
     1. Develop, in conjunction with The Authority, an automated, intelligent system for email distribution integrating with existing Authority systems to understand customer behaviour and target the next communication via the method that is the most effective for that customer/customer group using insight gained from customer behaviour.

## **CUSTOMER PORTAL**

* 1. From Day 1 the Supplier must:
     1. Provide a customer portal to allow customers to:
        1. Self-subscribe to and self-unsubscribe from email/SMS topics/categories that The Authority is willing to allow customers to opt in/out of;
        2. Manage their subscription;
        3. Update their name;
        4. Answer customisable questions; and
        5. Password protect their accounts (optional – not mandatory).
  2. From Day 2 the Supplier must:
     1. Consider the requirement for the platform to be linked into central customer portal operated by The Authority.
     2. Implement functionality for customers not to be able to opt out of certain communications the Authority is entitled to send.

## **MANAGEMENT INFORMATION (MI) REPORTING and DATA ANALYSIS**

* 1. The Authority requires available industry leading, accessible, accurate real-time, daily and on occasions ad-hoc MI covering core data all facets of the Service.
  2. The Supplier shall make available accurate daily and on occasions ad-hoc MI covering all facets of the Service offering to The Authority. For example:
     1. If fraudulent behaviour was observed, The Authority might ask for MI on the numbers used, which countries, how many times, duration of voice call (if applicable), which networks are used; and
     2. How many international SMS The Authority have sent over a given period of time, broken down by country.
  3. Specifically, for email and SMS campaigns:
     1. Using industry leading standard tools, core data must be able to be available via a shared portal, easily accessed and extracted by The Authority and be able to be configured and fed into analytic tools for analysis; and
     2. There is a future requirement for the Supplier to work with The Authority to automate and integrate MI data (including both delivery tracking data and next action tracking data) with Authority systems in the future, for both email and SMS. Option to configure and sending logging into SIEM. This will be a Day 2 activity.

## **REPORTING**

* 1. The Authority must have access on Day 1 to the following reports in both PDF and CSV format and with the facility for these to be generated by the user via the platform interface.
  2. From Day 2, MI and tracking will be automated, and different analytics/reporting frequency with/without the ability to pull manual reports will be required, the Supplier will work with The Authority to develop this requirement.
  3. MFA REPORTS
     1. The Supplier must provide callback notifications to provide The Authority with the success or otherwise of the delivery of the MFA SMS or voice request. Appendix – 1
     2. The Supplier shall make available accurate daily and on occasions ad-hoc MI covering all facets of the Service. For example:
        1. If fraudulent behaviour was observed, The Authority might ask for MI on the numbers used, which countries, how many times, duration of voice call (if applicable), which networks are used; and
        2. How many international SMS The Authority have sent over a given period of time, broken down by country.
  4. EMAIL REPORTS
     1. Email Analytics - with the ability to be able to select any of the following:
        1. Delivery Reports,including**:**
           1. Sent Date
           2. Bulletin Subject
           3. To
           4. Sender
           5. Delivery Status
           6. Total Recipients
           7. Total Delivered
           8. Total Failed
           9. Percent Delivered
           10. Bulletin Links Included
        2. Next action tracking, including:
           1. Unique Email Opens
           2. Unique Email Open Rate
           3. Total Email Opens
           4. Click Rate on hyperlinks included in emails
           5. Unique Bulletin Link Clicks
           6. Total Bulletin Link Clicks
           7. Shared Bulletin Page Views
     2. Recipient detail reports, with overview analytics of:
        + 1. Total emails sent
          2. Delivered
          3. Pending
          4. Bounced
          5. Unsubscribed
     3. Subscriber Reports - with the ability to be able to select any of the following:
        + 1. Date
          2. Total Subscribers
          3. New Subscribers
          4. Deleted Subscribers
          5. Total Subscriptions
          6. New Subscriptions
          7. Deleted Subscriptions
          8. Subscriber Change
          9. Subscription Change
     4. Topic Reports – with the ability to be able to select any of the following:
        + 1. Topic Name
          2. Topic ID Code
          3. Visibility
          4. Total
          5. Subscriptions to Date
          6. New Subscriptions to Date
          7. New Subscriptions this Period
          8. Deleted Subscriptions to Date
          9. Deleted Subscriptions this Period
          10. Bulletins Sent this Period
          11. Total Bulletins Sent to Date
          12. Date of Last Send
          13. Engagement Rate
          14. Sent Bulletins Clicks
     5. Category Reports - with the ability to be able to select all of the following:
        + 1. Category Name
          2. New Subscriptions to Date
          3. New Subscriptions this Period
          4. Deleted Subscriptions to Date
          5. Deleted Subscriptions this Period
          6. Total Subscriptions to Date
  5. SMS REPORTS **-** the ability to be able to select any of the following:
     1. Delivery data (including):
        1. Date SMS was sent
        2. Time SMS was sent
        3. Phone number SMS sent to
        4. Sent Yes/No
        5. Delivered Yes/No
        6. Message Content/wording
        7. Delivery Receipts
        8. Cost
     2. Next action tracking data:
        1. Clicks on hyperlinks included in SMS sent
     3. HLR (or alternative) dead number reports:
        1. Date HLR check performed
        2. Time HLR check performed
        3. HLR check result Live/Dead
        4. Cost
  6. Data encryption/retention
     1. Currently for SMS campaigns the telephone number is encrypted and shows as such on reports after 60 days (with the option to change to 30 days, 60 days, 90 days, 120 days if The Authority wishes). No encryption process in place currently for email. Data encryption/retention terms to be agreed between the Authority and the Supplier (see Section 37 – Data Storage).
  7. FOR BOTH EMAIL and SMS:
     1. The Authority must be able to:
        1. Report by date or selected date range as selected by the user, on all of the above reporting parameters outlined, both per individual campaign and across all email/SMS campaigns/HLR checks;
        2. Where campaigns have been ‘phased’ or issued as ‘batches’ there must be an option for the reports from each ‘phase’ or ‘batch’ to be combined and displayed as a single report, so as to avoid manual intervention to do so;
        3. Retain:
           1. copies of the emails/SMS sent;
           2. recipient list; and
           3. all analytical data as detailed above for a minimum of 12 months.
        4. Request all data is securely deleted/encrypted from the Supplier’s platform after a prescribed period.

* + 1. The Authority must also have access via shared portal to:
       1. Account Reports – Account performance; and
       2. User admin details, clearly showing individuals and their allocated roles/accesses
  1. The Supplier must report on all currently deployed patch and operating system versions against ALL relevant software/hardware (operational, support and administrative), along with current published versions and vendor support dates.  The report should also include details of any security vulnerabilities against the versions deployed along with associated risks to the current deployment and linking to any relevant remediation plans.

## **TRACKING**

* 1. The Authority requires the ability to utilise ‘tracking pixels’ in emails, to provide additional detailed analytics, including but not limited to:
     1. Delivery status;
     2. Email opens – unique and total; and
     3. Email link clicks – unique and total.

## **TRAINING AND GUIDANCE**

* 1. The Authority requires the solution to be designed as intuitive and user-friendly to use and navigate as possible, thus avoiding the need for lengthy detailed technical training for users.
  2. The Supplier must provide:
     1. On-site or virtual face to face training on the full end to end operation of all elements which will be operated by The Authority. This must be carried out in a controlled environment, before moving to the live testing phase;
     2. Programme of continuous training (and accreditations, where possible) for key users throughout the lifecycle of the contract;
     3. End to end training manuals, help cards, flowcharts etc;
     4. Updated guidance on any updates to System, Hardware and/or Software etc., when required; and
     5. Built in Contextual help from Day 1 (help buttons containing relevant information for that function/task) for every aspect of the software functionality.

## **DATA ANALYSIS / PREVENT RISK OF FRAUD**

* 1. The Supplier must:
     1. Use Data Analysis to detect and prevent fraud/bad behaviour where SMS is being exploited;
     2. Allow The Authority to conduct its own data analysis, the Supplier must provide:
        1. An Online Dashboard Service, showing delivery rates per country/network of both Voice Calls and SMS to a minimum fifteen (15) minute period;
        2. The ability to receive delivery information of SMS and Voice Call messages by API, to include Status codes/delivery failure/delivery confirmation: and
        3. Tools/analytics to detect and prevent fraud/bad behaviour where SMS and Voice Calls could be getting exploited for example (but not limited to) notification of any.
     3. Report a spike in requests to countries that either never request MFA or normally request very low volumes; and
     4. Report ‘ranges/blocks’ of numbers requesting MFA codes be sent to them.

## **INFRASTRUCTURE**

* 1. The Authority requires a system infrastructure consisting of a minimum of two (2) locations, based in the UK, which must be accredited with UKAS ISO-27001, ISO14001, ISO-9001, ISO18001. Each location will be accessed by a discrete internet addressable domain. There must not be one domain balanced across all locations. Two is the preferred number of locations.
  2. The Supplier will ensure that:
     1. All locations are run in an active – active mode to give The Authority surety that in the event of a failure of one location the service will continue to run seamlessly: and
     2. Each System Architecture has built in redundancies within the infrastructure for email, SMS and Voice Calls and therefore provide a 24/7, 365/366-day service without an unscheduled outage. Evidence of this to be supplied in the architecture diagrams supplied in the response.
  3. Where appropriate, The Authority will fully outsource particular services using Software as a Service (SaaS) to avoid infrastructure considerations entirely. All SaaS services will be subject to standardised security assessments as part of the on-boarding process. There should be alignment with The Authority’s security standards. Data should be uniquely encrypted, and The Authority would prefer to bring its own keys. Supplier staff should either have no access to The Authority’s data or be SC cleared.
  4. The solution must:
     1. Be hosted in the UK;
     2. Meet the required SLAs and NFRs, including HA and fault tolerance (see Section 44.1 – Fault Response);
     3. Be accessible and controllable in a programmatic fashion;
     4. Support utilisation based charging;
     5. Support the open telemetry standards to enable monitoring;
     6. Have appropriate protections against external attacks (DDoS, SQL Injection, etc.); and
     7. Support VPN connectivity for integration.
  5. Data must be:
     1. logically separated between customers; and
     2. be uniquely encrypted per customer.
  6. Security logs must be searchable, actionable and exportable to external systems.
  7. Any VPN IPSEC connectivity should support the NCSC PRIME standards.
  8. Service interactions within the solution Platform will be traceable and should be monitored end to end.

## **INTEGRATION**

* 1. The solution should support out of the box integrations with relevant systems (e.g. Service Desk, ServiceNow, Splunk, AzureAD, SAP, Pega, Office 365).
  2. The solution should integrate with Secure Data Exchange Services if required.
  3. The aim is to build on existing capability previously introduced through other digital services. The service can be adapted and enhanced to accept email, paper and SMS preferences depending on the Regimes/Services requirement to provide a contact service.
  4. The first iteration of the solution design details the IT components required for:
     1. Capture an Individual email Preference;
     2. Customers to set a digital or paper preference;
     3. The solution design will outline what needs to be implemented, enhanced and the building blocks that move The Authority towards the Strategic Preference Service Solution; and
     4. Project backlog requirement.
  5. Future contact preference work packages:
     1. Organisation Preferences.
     2. SMS.
     3. Braille.
     4. Mobile App.
     5. Welsh (TBC).
     6. Large Print.
     7. 3rd Party APIs.
  6. There is a requirement that the provider aligns to these strategic Coms channels. The Authority will store SMS preferences and data which could support its Campaigns etc. This is potentially a day 2 requirement, but the provider must have ability to perform a Pre-Check the number resides in the UK and is valid.
  7. Open API integration with 3rd party CRM applications.
  8. Current DES API’s – uplift to IF or waivers.
  9. Integration with Tel Com provider - Advisor UI, SMS service should have open APIs to integrate with any native or CRM application – via IF.

## **INTEGRATION WITH QUADIENT (Day 2 requirement)**

* 1. The Authority will be seeking in the future to integrate services with its Output Orchestration Service hosted on Quadient and therefore will require the Supplier to provide:
     1. Back-end RESTful API capability to allow external systems to submit requests of a prescribed format.
     2. API to include element for HTML content for email body and accompanying metadata created by external systems.
     3. API to include element text content for SMS messages created by external systems
     4. failure and success HTTP responses for 100% integrity.

## **EXISTING ARCHITECTURE**

* 1. The email and SMS communication platform will form part of a wider engagement ecosystem and must be capable of integrating with other systems, such as the telephony system, as per the Architecture diagrams below.



* 1. Customer Engagement Platform
     1. The email and SMS service that are the focus of this proposal are positioned within a broader omni-channel architecture vision that seeks to transform outcomes for The Authority and its customers. Key to this vision is a central architecture service concept referred to as the Customer Engagement Platform;
     2. Whilst the view of the technology service mix that The Authority will use to implement the Customer Engagement Platform is still forming, and indeed, is expected to continually evolve over the lifetime of the service; the mission of platform is clear. It will deliver the services required to maximise relevance in every customer contact and ensure consistent, context-aware interactions that deliver good, and ever-improving outcomes, for The Authority and its customers;
     3. The architecture components encapsulated within the Customer Engagement Platform are characterised by customer event logging, customer behavioural data, customer outcome data, predictive and adaptive analytics, rules engines and machine learning models driving intelligent automation across channels;
     4. It is expected that telephony and voice services set out in this proposal will be delivered ahead of the Customer Engagement Platform, so whilst suppliers cannot rely on integrating with its capabilities on Day 1, they should design their offerings in anticipation of a range of intelligent personalisation, and cognitive decisioning services emerging within the lifetime of the service, Day 2; and
     5. Note that Authority has adopted Pega Customer Service as the basis for its primary adviser user interface and requires that Supplier solutions integrate with this Adviser UI service. Looking forward, Pega ***may*** also be used to provide some aspects of the Customer Engagement Platform so it would be helpful if suppliers were to highlight any experience, they have of integrating with Pega.
  2. Digital Engagement Platform
     1. The Digital Engagement Platform provides webchat, asynchronous messaging, and virtual assistant and intent classification services for customer interacting online.
  3. Telephony Platform
     1. The Telephony Platform consists of a Core Telephony Service, Voice Automation Service and Call Recording & Speech Analytics Service; the platform provides automated customer voice journeys, self-serve applications, agent desktop, intent classification and intelligent call routing. Our Voice Automation Service also can channel shift customers to Web Chat via an SMS. On our telephony roadmap we aim to; offer customers informational SMS messages from appropriate IVR Journeys, we want to investigate the possibility of allowing our agents to issue SMS messages from the Agent Desktop likely using templates, and we may want to issue automated conversational SMS surveys to our telephony customers.
     2. Our Telephony Platform will require the Representational state transfer (REST) data transfer protocol to be made available in order to integrate with you to send SMS messages*.*
  4. Advisor UI
     1. This service is being supplied by Pegasystems Inc (Pega) and is the Pega Customer;
     2. Service (Version 8.4), also known as Pega Adviser UI. It will be deployed to around 30,000 agents;
     3. The Advisor User Interface (UI) will be used by agents to answer calls from the public and service their requests. The telephony solution will be required to integrate with Pega Adviser UI via the Pega Call Adapter. As a customer is routed to an agent via the telephony platform, critical information is populated from telephony integration and interactive voice responses into the Adviser UI (using Pega Call integration). IVR details collated (such as intent, authentication outcome, transcription of dialog with speech automation) will be passed to the Adviser UI Platform, along with references to the recording and/or the transcriptions of the adviser dialog, to ensure these can be easily linked to from the contact record;
     4. Telephony Integration with Pega is via Pega Callwhich supports both local and remote CTI links. With Open CTI Support, Pega Call supports three types of connectivity;
     5. Open CTI Server: allowing support for full or simple telephony with agent state management from within a Pega application;
     6. Open CTI Client: CTI integration at the desktop. Other integration options; and
     7. Native web call controls: Pega supports the ability to embed web call controls directly into the Pega Interaction portal.
  5. Application Access



* + 1. The document scope covers:
       1. Overview of background knowledge required to better understand the content;
       2. A high-level view of the current Authority internal networks and their disposition;
       3. A high-level view of the challenges presented by allowing external access to internal applications; and
       4. A discussion of how third-party users could access the services and applications using SSO to authentication and authorisation.
  1. Management Information & Business Insight
     1. The Authority is creating an omni-channel Management Information and Business Insight Service. The Supplier solutions should be capable of exporting operational and customer experience data for consumption by this service.
  2. Workforce Management
     1. The Authority is currently reviewing its requirements and ongoing need for Workforce Management services – Aspect provide and host the current capability. Suppliers should be prepared to integrate with industry standard historic and real-time interfaces with the The Authority’s Workforce Management platform.
  3. Integration View
     1. The diagram below illustrates the primary interface anticipated between the Email and SMS service in scope for this procurement. Adjacent Authority services are shown in yellow shaded rectangle.



|  |  |
| --- | --- |
|  | Administrative interface for reporting |
|  | Voice to Softphone endpoint |
|  | Adviser call recording pause and resume for manual credit card payments (not part of this procurement) |
|  | Call Search and Replay |
|  | Data export for journey and experience analytics |
|  | Voice recording / transcription archive |
|  | (Pega)CTI event to drive screen pop |
|  | Batch load of campaign to dialler |
|  | Voice Verification for a digital user |
|  | Intra-day and end of day files for WFM |
|  | Dialler published CTI event |
|  | Inbound telephony published CTI event |
|  | Write to Contact History (Pega) |
|  | Personalisation request (Voice automation API call to Pega, multiple scenarios) |
|  | PCI compliant card payment details |
|  | Identity: Request for Knowledge Based Challenge data set |
|  | Identity: Identity Verification result |
|  | Automated SMS to SMS Gateway |

## **IDENTITY**

* 1. For the avoidance of doubt this section **does not** apply to the MFA service.
  2. The Authority’s staff should authenticate to services via their primary identity provided by The Authority’s Azure Active Directory instance. This should preferably use OAuth 2.0 and OpenID Connect. SAML is acceptable as an alternative should OAuth 2.0 not be supported or meet the requirements.
  3. Services should externalise authorisation, preferably through the use of AzureAD groups. Alternative patterns for externalising authorisation to The Authority’s role-based access control systems may be acceptable to The Authority but must be agreed in writing by The Authority.
  4. Identities authorised to use the services that are not part of The Authority’s identity domains may require additional controls such as multi-factor authentication and must be agreed with The Authority in writing.
  5. The product should support externalisation of role allocation e.g. through use of SCIM.
  6. The product should support a method of provisioning user data.

## **CONNECTIVITY**

* 1. Data will be exchanged between The Authority and The Supplier using a secure electronic link of a type approved by The Authority. The Authority's current connectivity standard is via encrypted internet traffic (HTTPS, minimum of TLS 1.2. Other connectivity technologies may be acceptable to The Authority but must be agreed in writing by The Authority.
  2. The Supplier must:
     1. Provide any hardware and/or software that it may need in order to implement the agreed electronic link to The Authority, and such hardware and/or software must be compatible with The Authority’s system;
     2. Configure such hardware and/or software for the electronic link in order to be fully compatible with The Authority’s system;
     3. Exchange digitised content between The Authority and the Supplier via a secure link in the prescribed format using RESTful APIs with JSON payloads (see Appendix - 1);
     4. Provide a test service. The test service will require separate credentials, to enable The Authority to confirm the integration works and to assure itself that SMS and Voice Calls have been delivered;
     5. Ensure that the maximum response time for outgoing (from The Authority to the Supplier) requests does not exceed two (2) seconds. The preferred response time is less than 1 second. The notification requests from the Supplier to The Authority are asynchronous and are not subject to maximum response time;
     6. For the MFA service, ensure a minimum transfer rate of sixty (60) Transaction per second (“TPS”) for SMS and one (1) TPS for Voice Calls and a current maximum of one hundred and fifty (150) TPS for SMS and five (5) TPS for Voice Calls; and
     7. Detail the connectivity requirements of the solution, the protocols used and the ports utilised.

## **CUSTOMER ACCESS**

* 1. Customer access to user interfaces should be browser based, without the need for plugins.
  2. The service should work on mobile as well as desktop/laptop/tablet and supports.
  3. User interfaces need to be Web Content Accessibility Guidelines (WCAG) 2.1 compliant for accessibility standards.

## **SECURITY**

* 1. The Authority is a prime target for criminal phishing activity. It is vital that The Authority’s customers can trust the emails and SMS’s it issues through this service. It is critical for the service to maintain Customer confidentiality.
  2. The Supplier must:
     1. Have the ability to protect and report against phishing /smishing /vishing and work with the CST Customer protection team. Supplier to provide evidence to support this. For example, ability to check if mobile number is valid and not spoofed;
     2. Ensure that they comply with these relevant essential requirements throughout the term of the contract:
        1. UKAS ISO-27001 Certification;
        2. Cyber Essentials Plus Certification;
        3. CHECK approved Pen Testers on an annual basis or such time as both Parties agree, for both internal and external system IP’s. Tested to OWASP latest guidelines; and
        4. Cyber Risk Insurance.
     3. Have a Security Patch Management System;
     4. Ensure there are security controls in place to monitor, detect and prevent anomalous or unauthorised activity within their premises or environment. In the event of breach, The Supplier will take all reasonable measures to remediate the position whilst informing The Authority within a maximum of twenty-four (24) hours of detecting such anomalous or unauthorised activity within their premises or environment;
     5. Ensure they have a Privacy and Security Incident Response Plan, which undergoes six (6) monthly reviews and testing. This plan must always be kept current;
     6. Provide cyber security protection including but not limited to DDoS protection;
     7. Ensure their Data Centre’s are based in the UK with no data leaving the UK and should be situated in different locations to protect against service outage should anything happen to a Data Centre based in one location;
     8. Ensure that Data is be encrypted at rest. Ideally this will be AES256 or equivalent;
     9. Ensure that Data is encrypted in transit. This will be to at least TLS 1.2; and
     10. Ensure all user actions and automated system actions are logged to ensure security is not compromised.
  3. The Authority should be able to bring its own encryption keys.
  4. From a fraud protection/investigation side it is critical that the audit events/any delivery messaging available from the Supplier’s API continue to be ingested into Transaction Monitoring (as they are for the current Supplier). The specification of any audit events will be provided by the Supplier by The Authority and any changes to specification/format will need to be checked and fed into The Authority’s Transaction monitoring teams to ensure the correct events remain captured and surfaced.
  5. Continue not to use ‘alpha tags’ in SMS messages without prior contact/discussion with The Authority, whilst we can protect c90% of The Authority branded tags, The Authority are still steering away from their use – this to make the Supplier aware of the work in this space.
  6. The Supplier to provide visibility of details of authorised deliverers used to help The Authority with investigations into fraudulent activity.

## **SYSTEM ACCESSES AND CONTROLS**

* 1. The Supplier must provide:
     1. User friendly facility to set, control and manage user access to the platform, potentially through integration and single sign-on;
     2. Unlimited platform users; and
     3. Definable ‘administrator’ levels.

## **DATA STORAGE**

* 1. Data held on the platform must be securely stored with access to only a limited number of individuals.
  2. Supplier staff should have no access to customer data, other than telephone numbers used as part of the service, for investigative purposes only.
  3. Data should be encrypted at Rest with Certificates and encryption conforming to the level of data being processed and current Authority, government and NCSC standards.
  4. Information Lifecycle Management policies should be implementable for all data retained within this product. Data must be available to The Authority to manage to ensure it is kept for no longer than is necessary in accordance with Data Protection Act and GDPR.
  5. The solution should support a mechanism for mass export of data via an industry standard format (JSON, MYSQL, etc.).

## **AUTHENTICATION**

* 1. The Supplier must:
     1. Ensure that BASIC authentication, as a minimum, is provided on the requests from The Authority; and
     2. Be prepared to use static IP addresses that can be added to the “allow list” by The Authority to enable notifications to be sent back to The Authority. The Authority will supply the delivery or notification URL to use for the call-backs on each message sent to the Supplier. No authentication is required on the delivery/notification calls. The request is made over TLS 1.2 or higher to The Authority’s endpoints from “allow-list” IP addresses.

## **SOFTWARE UPDATES AND SOFTWARE MAINTENANCE**

* 1. The Supplier must ensure that:
     1. Any routine maintenance takes place outside of The Authority’s standard operating hours and must not incur any downtime whatsoever of the service i.e. must be non-disruptive;
     2. All software updates take place outside of peak periods, especially January, and as outlined in Section 10 - Volumes, unless critical in nature when any deployment must be agreed in advance with The Authority, who will not unreasonably withhold their permission;
     3. Any software updates must be planned in advance, tested and signed off by The Authority before going live, such permission will not be unreasonably withheld;
     4. There is an option to regress if an update fails in the live environment;
     5. In the event of an unsuccessful update, they consult with The Authority within 1 working hour and agree remediation activities to restore service; and
     6. Security patches are applied as soon as possible but no later than N-1.

## **SERVICE RESILIENCE**

* 1. The service must:
     1. Be designed to be resilient enough to cope with Business Continuity (BC)/ Disaster Recovery (DR) type scenarios;
     2. Robust service resilience must be designed into the service both technically and within the Supplier’s support models; and
     3. Be supported by an agreed BCDR Plan, which undergoes 6 monthly reviews and testing.
  2. The Authority must be satisfied that the Supplier can manage a BC/DR situation, however the requirement is for the solution to be designed to be resilient, thus avoiding the need for the BR/DR plans having to be invoked at all.

## **IMPLEMENTATION PLAN/MIGRATION**

* 1. The Supplier must:
     1. provide an implementation time line plan as part of its bid response (assuming migration to commence 1st Feb 2021); and
     2. Include a phased approach in its implementation plan and consider as a minimum the full integration of the Service with The Authority’s IT infrastructure, including supplying and building the infrastructure for outbound connectivity.
  2. The Supplier must work with The Authority to migrate:
     1. The existing database of c. 8 million email addresses, split into their relevant categories and topics, and ensure similar configuration on the new platform;
     2. Existing templates for email and SMS, if required by The Authority (to be decided at a later date); and
     3. Existing campaigns currently operating via API connections, including:
        1. CAMPAIGN A: one robotics campaigns for SMS (that also includes a hyperlink)
        2. CAMPAIGN B: an SMS campaign integrated with The Authority’s telephony system via API, see Appendix 2 for detail, additionally for Campaign B, the following controls would be applied on the platform:

|  |  |
| --- | --- |
| **Control** | **Value** |
| Mobile number Restriction | UK only |
| SMS limit per day to the same number | 10 |
| Sender ID | The Authority’s Campaign ID |

(Note: no APIs are currently used and need to be migrated for uploading email data)

* 1. Any change to the proposed operational go-live date must be subject to formal written agreement by both Parties.

## **SUPPORT SERVICE REQUIREMENTS**

* 1. SUPPORT SERVICE OPERATING HOURS
     1. For MFA and Multi Device Messaging: The Authority requires the platform to be available for messaging, self-service applications and configuration changes 24 hours per day, 365 days a year (366 days in a leap year); and
     2. For email and SMS campaigns: The Authority requires the platform to be available 7am to 9pm Monday to Friday (and occasionally at other time by agreement at no additional charge, giving 12-hours’ notice).
  2. The Supplier must provide:
     1. A dedicated Helpdesk (telephone) and specific contact points (email)/escalation routes for The Authority to contact in order to resolve customer issues such as, but not limited to the following:
        1. Non-receipt of SMS / Voice calls
        2. Non-receipt of email;
        3. Networks blocking traffic; and
        4. Any outages that disrupt the service
     2. Real time response to any instances where the service is unavailable and dedicated contact person(s) to manage this through to resolution; and
     3. A support function (Service Desk) must be available Monday to Friday to investigate MFA issues that customers raise with The Authority and which The Authority have raised with the Supplier. The Supplier must respond to The Authority’s Service Desk within 24 hours, Monday to Friday.
  3. The Authority’s **Help Desk** standard operating hours for enquiries for a normal working day are outlined in the below table.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** | **Sunday** |
| 08:00 to 17:00 | 08:00 to 17:00 | 08:00 to 17:00 | 08:00 to 17:00 | 08:00 to 17:00 | Closed | Closed |

* 1. The Authority’s **Service Desk** standard operating hours for enquiries for a normal working day are outlined in the below table.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** | **Sunday** |
| 08:00 to 18:00 | 08:00 to 18:00 | 08:00 to 18:00 | 08:00 to 18:00 | 08:00 to 18:00 | Closed | Closed |

* 1. Out of hours support is 18:00 – 08:00 for  P1 and P2 Events out of business hours 24 hours per day, 365 days a year (366 days in a leap year).

## **PRIORITY LEVELS**

* 1. Problems reported by The Authority will be allocated a priority level in accordance with the severity of the problem.
  2. A priority one (P1) problem consists of a fault which renders the whole or an important part of the service unavailable. This applies to the total outage of the Service or rejection of more than twenty percent (20%) of incoming order from The Authority’s interface due to service failure.
  3. A priority two (P2) problem consists of a fault causing acute operational problems creating significant business impact (e.g. considerable service restriction like the rejection of less than twenty percent (20%) but more than five percent (5%) of incoming orders).
  4. A priority three (P3) problem consists of a fault which causes non-acute operational problem (e.g. delays in sending the SMS to the Mobile Operator or unavailability of the Service Details-Extranet).
  5. A priority four (P4) problem consists of a fault causing Service Details-Extranet’s information to be partially inaccurate.

## **FAULT RESPONSE**

* 1. The Supplier must inform The Authority about any fault and to fix any reproducible fault within the following time frame.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stage/ Priority** | **P1** | **P2** | **P3** | **P4** |
| Initial response time | 15 minutes | 1 hour | 24 hours | 48 hours |
| Target Resolution (work around) | 30 minutes | 2 hours | 2 working days | Reasonable time |
| Target Resolution | 1 working day | 2 working days | Next release | Next release |

## **INVOICING**

The Supplier must provide monthly invoices to clearly show volumes within 7 working days from the end of the billable month end. The Authority is willing to discuss a flexible payment profile that might be monthly or quarterly in arrears.

* 1. The Authority requires unit charges against each element of the service, please refer to Pricing Table in Tender Documents.
  2. The Authority requires separate monthly invoice breakdowns for:
     1. MFA
        1. API connections
        2. SMSs
           1. UK
           2. Outside UK
        3. Voice Calls
           1. UK
           2. Outside UK
     2. Email campaigns
     3. SMS campaigns

Detailing usage and cost per campaign

* + 1. SMS alerts
    2. SMS:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Campaign name | SMS volume | HLR volume | SMS rate | HLR rate | SMS cost | HLR cost | Total |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Sub Total |  |
|  |  |  |  |  |  | VAT at 20% |  |
|  |  |  |  |  |  | Grand Total |  |

* + 1. Email:

|  |  |  |  |
| --- | --- | --- | --- |
| Campaign name | Email volume | Email  Rate | Total |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  | Sub Total |  |
|  |  | Grand Total |  |

The format detailed above (see clause 45.3) will prevail unless other terms are agreed between The Authority and the Supplier.

* 1. Invoices to be accessible to limited number of specified users with access rights via the User Interface for Campaign Management.

Invoices must include:

Invoice number

Invoice date

Payment due date

PO Number (to be supplied by The Authority)

The Authority’s name and address

Supplier’s name and address and contact telephone number

Month usage billed for

VAT registration number

Company number

Bank details:

Bank name

Bank Account name

Bank Account number

Bank Sort code

## **SERVICE & CONTRACT MANAGEMENT TEAM**

The Supplier must always provide a Representative / Service Manager / Contract Manager / Contract Management team to facilitate the business as usual activities associated with the Service, a named deputy should also be provided.

The Service Manager will liaise with The Authority’s Service Manager’s as applicable to ensure the smooth and efficient running of the Service.

The Contract Manager will liaise with The Authority’s representative/contract manager/contract management team as may be applicable given the nature and the extent of services required.

The primary contract management activity from both Parties will be to monitor, maintain and improve the service performance as detailed in Schedule 2.2.

To effectively manage the contract, both parties will contribute to, and agree, a formal contract management plan, as part of the implementation phase.

Contract Management will form part of the overall governance process. as referred to in Schedule 8.1.

* 1. As part of regular service reviews, the Supplier must provide at least 24 hours in advance:
     1. Performance data in respect of the required Service Level Agreements (SLAs) and Key Performance Indicators;
     2. Advice on new products that might be of interest to enhance our service or to protect against fraud attacks;
     3. Patching and updates as part of their regular service review; and
     4. Innovative options which would continuously improve the service and provide efficiencies in the processes, including the need to make improvements to accommodate any changes in legislation.

## **FUTURE DEVELOPMENT**

The Supplier must:

* + 1. Provide an outline of how much custom development/changes will cost and timescales and procedures for initiating and implementing;
    2. Be willing to work with The Authority in any future developments to feed email delivery information into The Authority’s systems;
    3. Have an exception process to respond more timeously if needed in times of peak demand, or for example in exceptional unpredictable circumstances i.e. COVID-19 pandemic.
  1. The product should provide Development Services and API Gateways that can be utilised by external development tools and services.
  2. The solution should provide configurable options for Release Management out of the box.
  3. If Release Management functions are provided the Solution should provide Packaging and Versioning Options out of the box.
  4. If Release Management functions are provided, the product should provide integration with Continuous Integration and Continuous Deployment Tools (such as Jenkins) out of the box.
  5. If Release Management functions are provided, the Solution should integrate with source code management tools (such as GitHub) out of the box for Package and Version Management.

## **APPENDIX 1**

The following are examples of the expected JSON messages that will be sent to either The Authority or the Sender:

Appendix x

These are example SMS messages sent to The Authority’s two providers. The key parts are the phone number to send to, the message and the delivery callback

{

"reqType":"BULK",

"MSISDN":"+447890123456",

"msg":"Your Government Gateway access code is 123456. Your code expires in 15 minutes",

"sender":"60886",

"delurl":"https://api.local.basgov.uk/delivery-details/supplier1",

"multi":true

}

{

"destinations":[

{

"to":"+447890123456"

}

],

"text":"Your Government Gateway access code is 123456. Your code expires in 15 minutes",

"notifyContentType":"application/json",

"notifyUrl":"https://api.local.basgov.uk/delivery-details/supplier2",

"from":"60886"

}

In both scenarios the response will have a unique reference that enables the callback to reference this request i.e. delivery notification

---------------------

This is an example of the voice request made. The key parts are the phone number to send to, the message, the language and the delivery callback

{

"destinations":[

{

"to":"+447890123456"

}

],

"text":"Your Government Gateway access code is 123456. Your code expires in 15 minutes",

"language":"en-gb",

"callTimeout":52,

"notifyContentType":"application/json",

"notifyUrl":"https://api.local.basgov.uk/delivery-details/supplier2",

"from":"60886",

"repeatDtmf":"1",

"dtmfTimeout":10

}

The response will have a unique reference that enables the callback to reference this request i.e. delivery notification

------------------------------------------

Supplier 1's example callback response

{

"reference":"32435543",

"MSISDN":"+448790123456",

"status":3,

"deliverytime":"2020-29-06 14:05:41"

}

Supplier 2's example callback response

{

"results":[

{

"bulkId":"80664c0c-e1ca-414d-806a-5caf146463df",

"messageId":"bcfb828b-7df9-4e7b-8715-f34f5c61271a",

"to":"+447890123456",

"sentAt":"2020-02-12T09:51:43.123+0100",

"doneAt":"2020-02-12T09:51:43.127+0100",

"smsCount":1,

"price":{

"pricePerMessage":0.01,

"currency":"EUR"

},

"callbackData":"User defined data.",

"status":{

"groupId":3,

"groupName":"DELIVERED",

"id":5,

"name":"DELIVERED\_TO\_HANDSET",

"description":"Message delivered to handset"

},

"error":{

"groupId":0,

"groupName":"OK",

"id":0,

"name":"NO\_ERROR",

"description":"No Error",

"permanent":false

}

},

{

"bulkId":"08fe4407-c48f-4d4b-a2f4-9ff583c985b8",

"messageId":"12db39c3-7822-4e72-a3ec-c87442c0ffc5",

"to":"+447890123456",

"sentAt":"2015-02-12T09:50:22.221+0100",

"doneAt":"2018-12-13T13:35:47.819+0000",

"smsCount":1,

"price":{

"pricePerMessage":0.01,

"currency":"EUR"

},

"callbackData":"reset\_password",

"status":{

"groupId":3,

"groupName":"DELIVERED",

"id":5,

"name":"DELIVERED\_TO\_HANDSET",

"description":"Message delivered to handset"

},

"error":{

"id":10,

"groupId":3,

"name":"EC\_BEARER\_SERVICE\_NOT\_PROVISIONED",

"groupName":"OPERATOR\_ERRORS",

"description":"Bearer Service Not Provisioned",

"permanent":true

}

}

]

}

## **APPENDIX 2**

