Service Terms & Conditions

These Service Terms & Conditions (“Terms” or “Agreement”) represent a binding agreement between KDDI America, Inc. (“KDDI”) and You. It is important that You understand Your responsibilities and the limitations to the Free Trial services which You choose to use. Our services are diverse and as a result additional service specific terms may apply. If this is the case, these service specific terms shall become part of Our agreement.

Please use Our services responsibly. By using Our website or any of Our services, You agree to Our Terms. Take note that these Terms change from time to time. If You have used Our services before, You cannot assume that the Terms are still the same. You should review them on a regular basis as the same will be published online with the date of the last change noted at the top.

1. Introduction

1.1. You wish to use KDDI services (meaning services as provided under these Terms; hereinafter “Service,” or the “Services”).

1.2. KDDI means KDDIKDDI AMERICA INC., a Corporation whose registered office is situated at 7 Teleport Drive, Staten Island, NY 10311, United States of America (hereinafter “KDDI”; “We”; Our”; “Us”).

1.3. You wish to use the Services and We are willing to make the Services available to You subject to and in accordance with these Terms

2. Binding Effect

2.1. You are entering into a binding agreement. If You accept these Terms of use of Our Service on behalf of Your employer or another person, You confirm that You have the consent of Your employer or that person to act on their behalf. THESE TERMS APPLY TO ALL RECORDS RELATING TO ALL TRANSACTIONS YOU ENTER INTO ON KDDI’S WEBSITE, INCLUDING NOTICES OF CANCELLATION, POLICIES, CONTRACTS, AND APPLICATIONS. In order to access and retain your electronic records, You may be required to have certain hardware and software, which are Your sole responsibility.

2.2. You are not eligible to accept these Terms or use Our Services if You are not of legal age to form a binding contract with Us or if You are barred by law to use Our services.

3. The Service

The Service enables a Customer to use Our mobile services as set out as part of Your online registration. Any such billable unit under the Services shall be referred in these Terms and Conditions as a “Chargeable Event”.

4. Availability and Interruption of the Service

4.1. We will make the Services available to You using reasonable skill and care. You do however acknowledge and agree that the availability of the Services, Your ability to access and/or use the Services and the conducting of any given Chargeable Event may depend upon factors beyond Our reasonable control, including (but not limited to):

- Factors affecting the operation of the Services and/or preventing Chargeable Event from being successfully conducted such as, by way of example, geographical or topographical shortcomings in the network of any telecommunications network operator (“Network Operator”), network capacity, physical obstructions or atmospheric conditions; or

- Factors preventing end-users from receiving Chargeable Events such as, by way of example, the terms and conditions of an end-user’s service provider.

4.2. We cannot therefore guarantee:

- That the Services will be available to You at all times or free from faults or interruptions;

- The receipt by any intended recipient of any Chargeable Event sent using the Services (as applicable).

4.3. We will not be in any way liable for any failure to make the Services available to You to the extent that such failure results from a technical or other failure on the part of any Network Operator or any other event which is beyond Our reasonable control. We provide all services “as is” and “as available”, and

We hereby do not warrant, represent or guarantee, whether expressly or by implication, that any Services are free of errors or interruptions, always available, fit for any purpose, secure or do not infringe any third party rights.

4.4. We may, at Our sole discretion, alter or improve the Services We provide to You at any time, provided that any such alteration does not materially affect the nature or detract from the functionality of the Services.

4.5. It may be necessary from time to time for Us to suspend the Services that We provide to You for routine or emergency maintenance and/or repairs and We will, in so far as it is reasonably possible, provide You with a reasonable period of notice prior to any such suspension.

- We may at Our sole discretion suspend Your access to the Services and/or cease to allow any Chargeable Events to be conducted by You at any time. We are entitled to terminate these Terms for any reason, in which case We will give You appropriate notice as soon as is reasonably possible.

- Should Your account utilized in the provision of KDDI Service be inactive through a period of 6 (six) months it remains in KDDI’s discretion to suspend KDDI Services to You. You can reactivate the account with a request to KDDI sent 3 (three) working days prior to the required reactivation.

5. Account, Passwords and Security

5.1. In order to provide Our services, We may require certain information. You must ensure that the information is complete and accurate. We may suspend or terminate any service if You give information that is not complete and accurate. You warrant that all information You provide to Us is complete and accurate and You indemnify KDDI against any liability that may arise as a result of Your failure to provide complete and accurate information. You must immediately notify Us if any of Your information changes.

5.2. We will provide You with a user name or customer ID or ask You to choose authentication credentials for each account. We may change, cancel or suspend Your account, which You will be notified about.

5.3. You:

- must keep Your username, customer ID, password, ApiKey, login token or any other secret authentication credential confidential;

- must not circumvent, or attempt to circumvent, Our user authentication systems;

- must inform Us immediately of any unauthorized use of Your account or any other breach of security, including suspected doubts of such scenarios;

- are entirely responsible for all payments and any activities that occur on Your account;

- are liable for any damage, loss or costs that we or any third party may sustain as a result of any of your actions, or any actiony use of Your authentication credentials, account name or account information by a third party or as a result of Your violation of this section.

- are responsible for authorized and unauthorized use of Your account in case any of the security recommendations (point 5.4) are not or had not been implemented from Your behalf at the moment of questionable activity on Your account (i.e. in scenarios where, due to Your inability to implement maximum security measures available at your disposal, a potential unauthorized activity had taken place). This includes (list not exhaustive): service login, subsequent data insight, sending messages traffic, payments. Responsibility for these activities includes assuming liability for any damage, loss or costs that KDDI or any third party may sustain as a result of these activities;

- must cooperate with Us during the resolution of potential unauthorized use of Your account, regardless of its cause and source of initial reporting.

5.4. You are mandated to follow Security recommendations (depending on the channels / Services used), available on Schedule 1. For any questions, as well as in case of security compromise of your authentication credentials (username & password, ApiKey), You should contact KDDI immediately via ms.support@kddia.com.

6. Confidentiality and Data Protection

6.1. You will at all times keep confidential all information acquired as a consequence of using Our Services, except for information already in the public domain or information which You are required to disclose by law, requested by any Regulator or reasonably required by Your professional advisors for the performance of their professional services. When using Our Services, you shall comply with all laws and regulations applicable to the use of the Services and with Our Terms or any other terms as agreed between us.

6.2. Please refer to Our Privacy Notice for details on personal data processing with respect to Our Services.

6.3. With respect to the processing of personal data of your end-users that you provide to us through our Services, You are controller and KDDI is processor. You guarantee that you have obtained all required and valid consents under the applicable data protection laws and regulations (such as the EU General Data Protection Regulation) as required for the processing of personal data by KDDI for the performance of our Services and KDDI will process that personal data only upon Your instructions and in accordance with data processing agreement. . If you wish to enter into a data processing agreement with KDDI you can send a request to privacy@kddia.com and we will provide you with a pre-signed version of our data processing agreement.

7. Support services

7.1. Unless We agree otherwise in writing, We will provide on-line technical support via email in respect of the Service available to You at the following e-mail address: **ms.support@kddia.com**

8. Customer Charges and Payment

8.1. If applicable and/or if otherwise stated in Your online Trial Application Form,You agree to pay all Charges due to Us in respect of making the Service available to You and Your access to and use of the Service ("Customer Charges") by the prepayment method and in accordance with the terms as set hereof.

8.2. If applicable and/or if otherwise stated in Your online Trial Application Form, You agree to pre-purchase credits for each month of the Agreement or such other period as is agreed between us, in which case We will allocate to You a corresponding credit. Each Chargeable Event that You conduct using the Service will therefore reduce the value of the credits available to You by the corresponding amount.

8.3. If applicable and/or if otherwise stated in Your online Trial Application Form,any change in prices that might occur for one or more destinations shall be communicated to You via email and/or noted on our website.

8.4. If applicable and/or if otherwise stated in Your online Trial Application Form, You shall be solely responsible, by seeking adequate Chargeable Event credit allocation(s) and checking Your remaining available Chargeable Event credit level on Our website, for ensuring that You have enough Chargeable Event credits to meet Your requirements from time to time and We shall not be in any way responsible or liable in the event that You have insufficient Chargeable Event credits to meet Your requirements, and/or have exceeded Your Chargeable Event credit allocation(s), for any period.

8.5. If applicable and/or if otherwise stated in Your online Trial Application Form, and for the avoidance of doubt, a Charge will be incurred for every Chargeable Event conducted by You regardless of whether it is successfully delivered.

8.6. If applicable and/or if otherwise stated in Your online Trial Application Form, and if You do not pay any Customer Charges in accordance with the applicable payment terms, We reserve the right to, in Our sole discretion, suspend Your access to the Service and/or cease to allow any Chargeable Event to be conducted by You until further payment is received by Us which fully covers any unpaid Charges.

8.7. If applicable and/or if otherwise stated in Your online Trial Application Form, You are responsible for the payment of all bank and finance charges. Please ensure that the amount received on Our bank account, after deductions, corresponds to the full amount you owe Us.

8.8. If applicable and/or if otherwise stated in Your online Trial Application Form, You will not be able to receive any refund for the payment made (“No refund, exchange only”). The latter shall not prevent any refund to be made according to the applicable customer protection laws.

9. Marketing

Parties hereby grant each other the right to use and display each other’s name and logo („Trademarks“) for promotional means on the respective websites or other promotional material, however, restricted solely in connection with the services provided under this Agreement. Any usage under this clause shall be done according to the proprietor Party’s guidelines as they may be provided from time to time. Neither Party shall use the other Party’s Trademarks in any manner that will disparage, harm or otherwise damage the other Party’s goodwill in its Trademarks. The Party using the Trademarks shall not, at any time, misuse the same or present itself as an affiliate or other legal agent of the Party whose Trademarks are being used. Any rights and linked usage of Trademarks granted under this Section shall be immediately discontinued in the event this Agreement is terminated.

10. Rules of Use

10.1. You warrant that You will not:

- Use the Services or permit the Services to be used to send Chargeable Events to any end-user for marketing purposes without that end-user's explicit request for, or prior consent, to receiving them. If you are sending any Chargeable Event for commercial purposes to any of Your end-users, You must abide by the telephone marketing practices of the end-users' jurisdiction, including but not limited to, obtaining prior express written consent from those end-users, and give all end-users the right to opt out of receiving any further Chargeable Events sent by You for commercial purposes (and You shall promptly process any end-user's election to opt out);

- Use the Services or permit the Services to be used to convey Chargeable Events to any end-user, with a frequency and in numbers which are excessive in Our reasonable opinion;

- Use the Services or permit the Services to be used for any improper, fraudulent, immoral or unlawful purpose;

- Use the Services or permit the Services to be used for the transmission of any material which is of a defamatory, offensive, illegal, abusive, obscene or menacing character or nature;

- Use the Services or permit the Services to be used in a manner that infringes the intellectual property rights or any other proprietary rights of any third party; or

- Use the Services or permit the Services to be used in a manner that may injure or damage any person or property or cause the quality of the Services to be impaired.

10.2. You will at all times during the duration of the Agreement:

- Send only Chargeable Events that comply with all applicable laws, regulations and Codes and that contain nothing which is likely to cause offense in view of the generally prevailing standards of decency and propriety from time to time;

- Comply with all reasonable directions and instructions issued by Us from time to time in relation to the Services;

- Comply with and observe at all times all applicable laws, regulations and Codes and any directions, recommendations and decisions of any Regulator; and

- Not act in any manner likely to bring Us, the Service or any Network Operator into disrepute.

10.3. You will, upon request, provide Us or any Network Operator or Regulator with any information relating to Your use of the Services that the requesting party reasonably requires. You are responsible for ensuring that any information relating to Your end-users, including (but not limited to) Your end-user Data, is accurate and complete.

10.4. You will not state or imply any approval by Us of any particular Chargeable Event that You send using the Services or refer to Us in any way without Our prior written approval.

10.5. Where requested by Us, You will promptly provide Us with a representative Forecast of Your Service needs for the requested period, including (but not limited to) all reasonable details required for Us to plan network capacity requirements.

10.6. We may, at Our sole discretion cease to convey, and You will promptly cease to transmit at Our request, any Chargeable Event.

10.7. You warrant that You are the sole owner or licensor of all rights in Your End-User Data or You have obtained all necessary rights, licenses and consents from all relevant third parties to enable You, Us and Our sub-contractors to use the End-User Data for the purposes of the Agreement.

11. Disclaimers, Limitations of Liability and Indemnification

11.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KDDI SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS OR REVENUES, WHETHER INCURRED DIRECTLY OR INDIRECTLY, OR ANY LOSS OF DATA, USE, GOOD-WILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM (i) YOUR USE OR THE INABILITY TO USE THE SERVICES; (ii) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES RESULTING FROM ANY GOODS, DATA, INFORMATION, CONTENT AND/OR ANY OTHER SRVICES OBTAINED THROUGH THE SITE; (iii) THE UNAUTHORIZED ACCESS TO, OR ALTERATION OF, YOUR

REGISTRATION DATA AND/OR VERIFIED PROFILE; AND (iv) ANY OTHER MATTER RELATING TO THE WEBSITE AND/OR THE SERVICES OFFERED ON THE WEBSITE.

11.2. THE LIMITATIONS OF THIS SUBSECTION SHALL APPLY TO ANY THEORY OF LIABILITY, WHETHER BASED ON WARRANTY, CONTRACT, STATUTE, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, AND WHETHER OR NOT THE KDDI ENTITIES HAVE BEEN INFORMED OF THE POSSIBILITY OF ANY SUCH DAMAGE, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

11.3. You agree to indemnify and hold KDDI, its officers, directors, shareholders, predecessors, successors in interest, employees, agents, subsidiaries and affiliates, harmless from any demands, loss, liability, claims or expenses (including attorneys' fees), made against KDDI by any third party due to, arising out of or in connection with your use of the website and/or the Services.

11.4. We will not be in any way liable for the content of any Chargeable Events sent or transmitted using the Service and the full responsibility for their content shall rest on you. You must observe all relevant legislation and regulations applicable in your jurisdiction and in the jurisdiction of all persons with whom you communicate directly when using the Service. By using the Service you also agree to be bound by the Rules of Use.

11.5. Notwithstanding the foregoing, You acknowledge you will be solely responsible for any legal liability arising out of or relating to the Content and Services (whether transmitted on your own or on any Third Party's behalf).

11.6. Subject to any express provision to the contrary in these Terms, We will not in any circumstances be liable to You in contract, tort, negligence or otherwise for any economic loss (including, but not limited to, any loss or profits, business, contracts, revenue, turnover or anticipated savings) or for any indirect or consequential losses, whether or not they were foreseen or foreseeable.

11.7. Each party acknowledges that neither You, nor We, have entered into the Agreement on the basis of or in reliance upon any representation (save for any representation made fraudulently), warranty or other term except as otherwise expressly provided in the Terms and, as such, all conditions, warranties and other terms implied by statute, common law or otherwise are hereby excluded to the greatest extent permitted by law.

11.8. We shall at all times in respect of the subject matter of these Terms comply with all applicable laws, regulations and rules having equivalent effect.

11.9. You shall be responsible for explaining and answering to any complaints that We receive from any relevant regulatory body resulting from your use of the Service. We will forward any complaints to you as soon as it is reasonably possible. You must follow the applicable complaint procedures and respond to each complaint within the timeframes specified by the relevant regulatory body and must forward a copy of your response to Us immediately. You will be liable for any fines and/or penalties imposed by any regulatory body against You or Us or any of our associated companies, due to Your contravention of these Terms.

12. Term and Termination

12.1. Either Party can terminate this agreement at any time by notice to the other Party with or without cause.

12.2. Either party may also terminate this Agreement with immediate effect by notice to the other party if:

- The other party becomes insolvent, makes any arrangement with or for the benefit of its creditors, goes into compulsory or voluntary liquidation, has a receiver, administrative receiver, liquidator or other similar official appointed over its assets, is subject to an administration or similar order or ceases trading;

- The other party commits a material breach of the Agreement and (where such breach is capable of remedy) fails to remedy the breach within 14 days of a written notice from the party not in breach requiring its remedy; or

- Any license required for Us to operate the Services is revoked, terminated or modified or, in the case of new license requirements being imposed, the applicable license: Is not granted to Us; or Is granted to Us but in such a way as to prevent Us from continuing to make the Services available or a Network Operator from enabling Us to make the Services available.

12.3. We may terminate the Agreement immediately upon notice in the event that any relevant legislation or regulation is implemented or modified with the effect that it is no longer commercially viable or possible for Us to make the Services available.

12.4. Termination of the Agreement for any reason does not affect any rights that have accrued to either party under the Agreement up to the date of its termination and those terms and conditions of the Agreement that are by their nature capable of surviving termination will continue in full force and effect following such termination.

12.5. On termination of the Agreement:

- You will immediately cease to use the Services; and
- If applicable and/or if otherwise stated in Your online Trial Application Form, all amounts then owed to Us, under or in connection with the Agreement, will become immediately due and payable.
- If applicable and/or if otherwise stated in Your online Trial Application Form, You will forfeit any unused credit on your account, except for payments received by us within seven (7) days prior to termination.
- All licenses and rights granted under these Terms will terminate immediately.

13. Force Majeure

Neither party will be liable for any delay in the performance of or any failure to perform any of its obligations under this Agreement that is caused by any event which is beyond its reasonable control, including, but not limited to, the failure, malfunction or unavailability of necessary telecommunications, data communications and/or computer services, power supply failures or shortages, acts or omissions of third parties (including, but not limited to, Network Operators), acts of government or Regulators or telecommunications network congestion.

14. Assignment

Neither party will assign, transfer or sub-contract either in whole or in part any of its rights or obligations under the Agreement without the other party’s prior written consent (not to be unreasonably withheld or delayed), provided that We shall be entitled without Your prior written consent to assign, transfer or sub-contract in whole or in part any of its rights or obligations under the Agreement to any affiliated company.

15. Intellectual Property

15.1. All content, trademarks and data on our website, including software, databases, text, graphics, icons, hyperlinks, private information, and designs are the property of or licensed to Us, and as such, are protected from infringement by domestic and international legislation and treaties. Subject to the rights afforded to You in these Terms, all other intellectual property rights on this website are expressly reserved.

15.2. We may grant You an individual, personal, non-exclusive and non-transferable license ("the License") to use our proprietary software or application service, in object code form only, and only in accordance with the applicable Service Specific terms and other documentation, if any, and only in conjunction with the relevant services. You may not reverse engineer, de-compile, disassemble or otherwise attempt to establish the source code or underlying ideas or algorithms of our software; modify, translate, or create derivative works based on the software or application; copy, rent, lease, distribute, assign, or otherwise transfer rights to the software or application; or remove any proprietary notices or labels with regard to our services. We retain ownership of all propriety applications, software, intellectual property and any portions or copies thereof, and all rights in it. You will notify Us of any suspected infringement of Our intellectual property of which You become aware and will take all reasonable action as We may direct in relation to that suspected infringement where such is directly and specifically related to the services we provide you.

15.3. These Licenses terminate when Our contract with you ends and you must destroy and stop using all of our software and applications in your possession. The software is provided and applications are offered "as is" and subject to the service warranty disclaimers and limitations of liability found elsewhere in these Terms. It is your responsibility to test the services before entering into this contract.

15.4. Content from Our website may not be used or exploited for any commercial and non-private purposes without Our prior written consent.

16. Severability

If any term or other provision of this Agreement is determined to be invalid, illegal or incapable of being enforced by any rule or law, or public policy, all other conditions and provisions of this Agreement shall nevertheless remain in full force and effect.

17. Governing Law & Dispute Resolution

This Agreement and Terms shall be governed by and construed in accordance with laws of state of New York, without reference to its provision on conflicts of law. The parties agree that any and all disputes and/or controversies arising out of, relating to, or in connection with this Agreement and any of its attached schedules and/or exhibits, or the termination thereof, or the interpretation, validity, construction, performance, breach, or termination thereof, shall be settled by expedited, binding arbitration to be held in New York City, New York in accordance with the National Rules for the Resolution of Commercial Disputes then in effect of the American Arbitration Association (the "Rules"). The decision of the arbitrator shall be final, conclusive and binding on the parties to the arbitration. Judgment may be entered on the arbitrator's decision in any court having jurisdiction. The arbitration proceedings shall be governed by the Rules, without reference to state arbitration law.

18. Summary Terms and Conditions:

You confirm that You hold the account corresponding to the data You have provided KDDI with, or that You have the account holder’s permission to use this service.

Schedule 1 - Security Rules and Recommendations

These Security Rules and Recommendations guidelines are meant to help you securely perform authentication and other user actions on the KDDI platform.

For easier navigation through the KDDI security essentials, take a few minutes to get familiar with the basic rules, including User Verification and Changing User Account`s Contact Information.

The next important part of this page involves recommendations where you can learn about password management, sharing confidential information, secure file transfers, and more.

User Verification

After a user account has been created, the traffic can`t be sent from this account without proper verification. Right after the login, the unverified user will see a pop-up message: “This user has not yet been verified to send traffic! Please contact your account manager for verification.“

The verification process pertains to the first time users of the client`s main account and any of the sub-account(s) in use that connects to the KDDI platform via our web interface and/or API.

Changing User Account’s Contact Information

New users are able to input and/or modify the GSM number and email address fields on the KDDI web interface during the first 7 days from the date the user account has been created. Modification of your own or other user’s contact details will be disabled after that date to ensure that authentication flows are not interrupted (2FA and/or email verification forms).

After input fields are disabled, users will see a pop-up message: “To edit GSM and email address, please contact your KDDI account manager or ms.support@kddia.com.”

Password Management

Security parameters can be adjusted under Account Settings on the KDDI web interface.

Increase Password Strength for ALL Users

There are 5 levels of password strength on the KDDI web interface that you will be able to choose from. Each has a description of associated parameters related to length and complexity. KDDI recommends using the *very strong* level (except where the protocol proprietary restrictions apply):

- Min length: 10
- Must contain alphanumeric characters [a-zA-Z0-9]
- Must contain a lowercase character

- Must contain an uppercase character
- Must contain a digit
- Must not contain the username
- Does not contain repeated characters
- Must contain non-alphanumeric characters

Follow these important password tips to help protect your account:

- Do NOT use the same password for different users
- Do NOT use passwords that you use elsewhere, especially for other online channels/services
- **CHANGE passwords periodically**, on a quarterly basis at least
- Set **Maximum Login Attempts to 5** to protect your account from brute-force attacks
- **NEVER share your passwords or API keys** with 3rd parties, including KDDI staff. Instead, use the KDDI web interface password reset form or manage API keys over the appropriate interface.

Entry Point-Specific Users

Use separate user accounts for HTTP/SMPP API and KDDI web interface access. Different security measures apply for each (explained in the paragraphs below).

IP Safelisting

IP safelisting allows you to create lists of trusted IP addresses or IP ranges from which human users or APIs can access the KDDI platform.

When using IP safelisting, please keep in mind the following conventions and best practices:

- IP safeliting on the user-level (regardless if used by a human user or API). This setting is available only to the KDDI administrators.
- Allowed IP ranges/individual addresses are applied on the user level only. This makes them applicable in the scenarios where **separate users are used for API and web interface logins**:
    - API – typically using static IP addresses or company/ISP ranges; a good option for IP safelisting features.
    - Web interface – might originate from dynamic source IP addresses (e.g., users working from home, connecting via mobile network or when traveling); use IP safelisting with caution.
- If you wish to set an IP safelist, provide a full range of IP addresses used for SMPP/HTTP API connectivity to your KDDI account manager.

- IP safelist set for users override the domain safelisting.

NOTE

IP safelist for HTTP API key and basic authentication are complementary (different restrictions apply, depending on the authentication method used).

API-Related Security Controls

This section provides information on how to increase security for API connectivity.

To mitigate the risk of network data transfer interception:

- Stop using a combination of unsecured HTTP and SMS over URL parameters due to a high risk of network data transfer interception.
- Stop using the unencrypted HTTP/SMPP connection and switch to the following:
  - SSL/TLS encrypted connections (**preferred option** due to a faster setup and more robust failover mechanism).
  - Contact ms.support@kddia.com for an IPsec VPN connection implementation (**less preferred** due to the need for manual setup and more complex incident management in case of availability issues).

  This will provide an encrypted data path between your platform and KDDI.
- Refrain from using GET methods for sending messages

To mitigate the risk of password abuse, use a time-constrained **API key or token authorization type**.

For more details on all of the above, refer to the articles on the KDDI API Developer Hub: Authentication and API Key.

API Key Validity

- API sessions expire one hour after the last successful token, and this option cannot be modified on the client's account level.
- API keys, on the other hand, are sessionless and sent with each request. They have a validity period that can be set per API key after which the API key is considered invalid/expired.

For more information on the API key model and how to update your API key, refer to our KDDI API Developer and API Key article.

Web Interface Related Security Controls

Two-Factor Authentication (2FA) is a cloud messaging security solution that confirms the identity of the user and protects the system from phishing or hacking attacks.

Once you set up the 2FA for the account, it affects all users.

NOTE

Enabling 2FA for user accounts using API will not impede connectivity.

To enable 2FA on the KDDI web interface itself, navigate to **Settings** > **Edit Account**, and use the toggle to turn two-factor authentication **ON**.

Verify the Authenticity of Login Page to Prevent Phishing Attacks

Pay close attention to the URL and site content:

Check Favicon. Websites can put whatever icon they want in the tab.

Look at the domain name. The domain name can help confirm that you are landing on a legitimate KDDI site.

Check the site's security status in your browser's address bar. For most browsers, a *safe* website will display a green padlock icon to the left of the website's URL. You can click the padlock icon to verify the details of the website (e.g., the type of encryption used). For example:

- Multiple dashes or symbols in the domain name.
- Domain names that imitate actual businesses (e.g., "KDD1").
- Domain extensions like ".biz" and ".info". These sites tend not to be credible.
- Keep in mind as well that ".com" sites, while not inherently unreliable, are the easiest domain extensions to obtain.

Check the website's connection type. The KDDI web interface website has an "https" tag which is more secure and therefore more trustworthy than a site using the more common "http" designation. This is because "https" sites' security certification is a process that most illegitimate sites would not bother with.

Look at the file path. KDDI web interface has straightforward file paths depending on the part of the web interface you want to visit. In case of any doubts related to the path, please contact our Support (ms.support@kddia.com).

Evaluate the URL. A website's URL consists of the connection type ("HTTP" or "HTTPS"), application (e.g., "portal"), domain name itself (e.g., "KDDI"), extension (".com"), and the file path (e.g. "/dashboard"). Even if you've verified that the connection is secure, remain on the lookout for the following red flags:

- The Favicon – websites can put whatever icon they want in the tab.

- Domain Name – this is a part of the URL and it's trustworthy, as long as you know what you're looking for.
- File Path/Director – this is a part of the URL and it's trustworthy, as long as you know what you're looking for.
- Web content area – this can be whatever the attacker wants it to be, including a very convincing spoof of an KDDI's legitimate website.

Look for broken English on the website. If you notice a large number of poorly-spelled (or missing) words, generally bad grammar, or awkward phrasing, you should question the site's authenticity. Even if the site in question is technically legitimate insofar as it isn't a scam, any inaccuracies in language will also cast doubt on the accuracy of its information, thereby making it a poor source.

Review Certificate details:

Most browsers allow you to view the certificate by clicking the padlock icon in the address bar.

For Firefox:

1. Click the padlock icon
2. Click **More Information**
3. Click **View Certificate**

For Safari:

1. Click the padlock icon
2. Click **View Certificate**

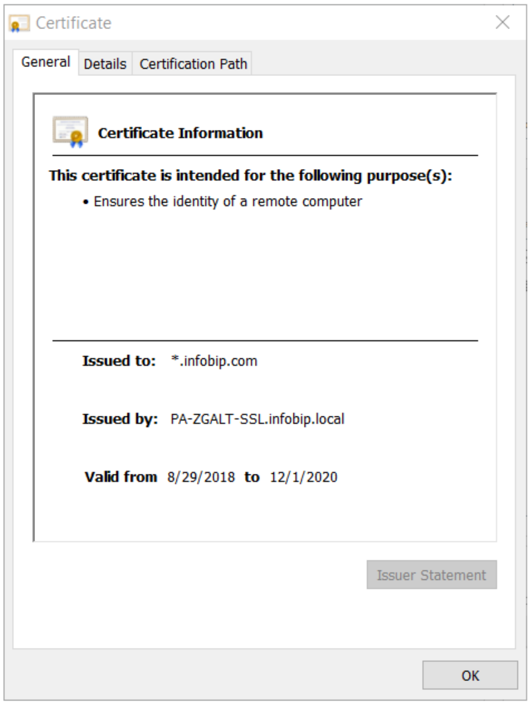
For Chrome:

1. Click 3-dot menu > **More tools** > **Developer tools**
2. Click the **Security** tab and **View certificate**.

-or-

1. Click the padlock icon > **Certificate**.
2. When you click the **Certificate Information**, you will get all the information the CA verified before it issued the certificate.

The KDDI certificate looks like this:



Certificate Information

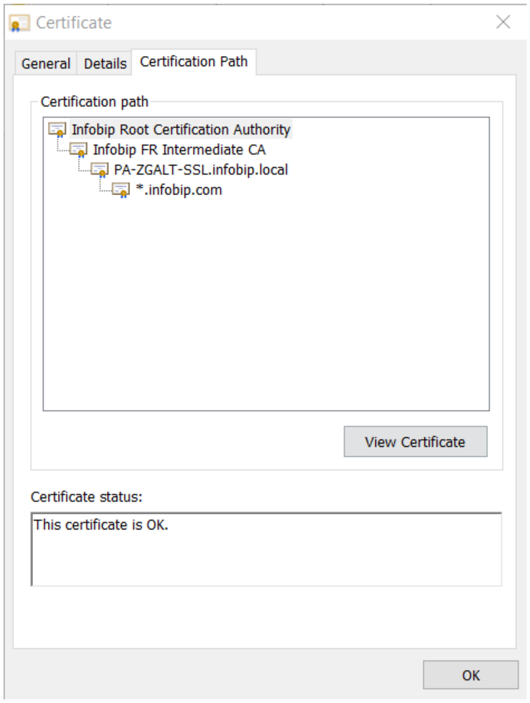
This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: *.infobip.com

Issued by: PA-ZGALT-SSL.infobip.local

Valid from 8/29/2018 **to** 12/1/2020



Certification path

```
Infobip Root Certification Authority
  Infobip FR Intermediate CA
    PA-ZGALT-SSL.infobip.local
      *.infobip.com
```

Certificate status:

This certificate is OK.

Sharing Confidential Information

This section is a quick guide on how to safely use and store confidential information.

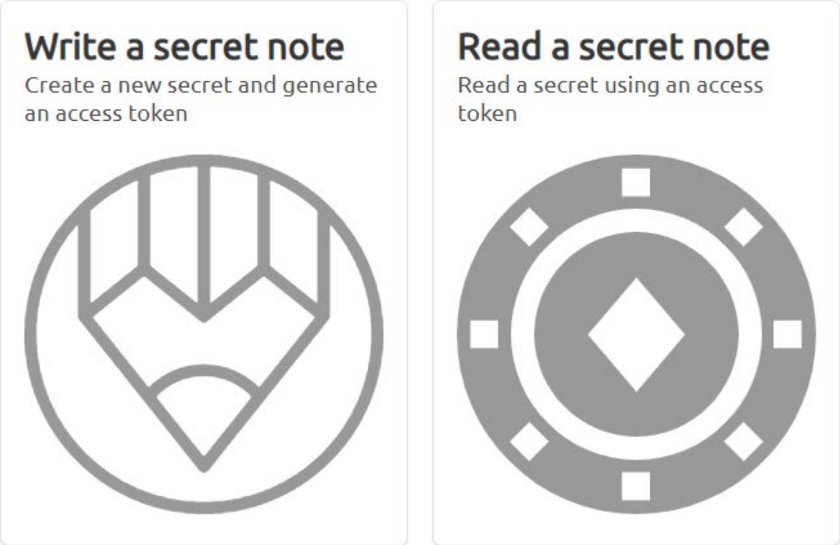
How to Use S-Pass

S-PASS is an KDDI **app for sharing confidential information with the KDDI employees, clients, and other 3rd parties.** Please note that **shared information is readable only once,** and then it is permanently erased from S-PASS.

It is possible to **create and send a secret note** to a recipient or **access and read a secret note** if you have received a token from the sender. In both cases, it is necessary to **access** https://s-pass.app/ using a web browser of your choice (it might look different in different web browsers).

Store a Secret

1. **Access** [S-PASS](https://s-pass.app/). Click **Write a secret note** to share a secret with someone or **Read a secret note** if you have received a token for reading secret notes.



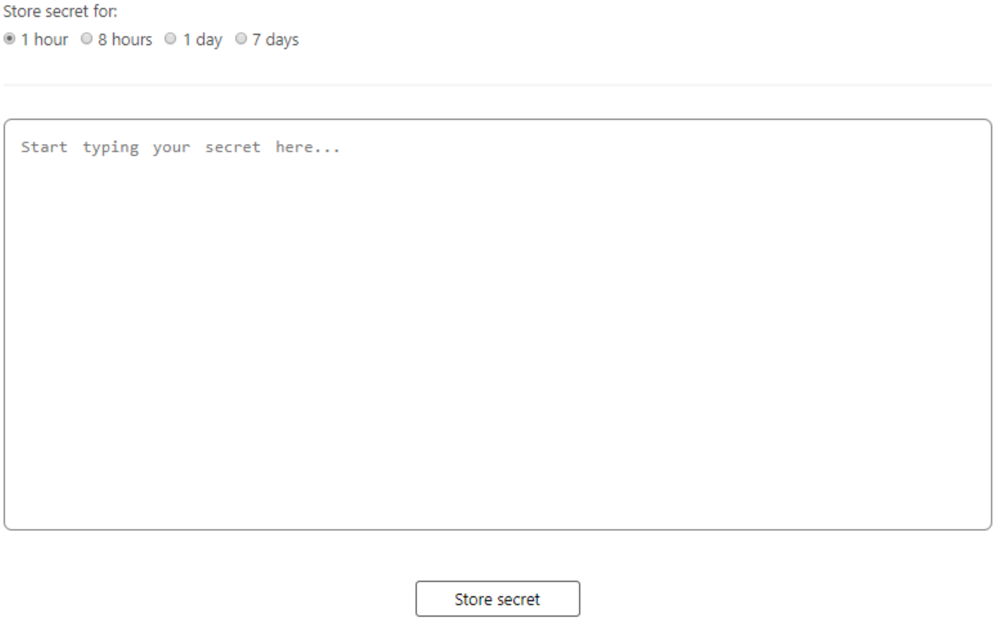
Write a secret note

Create a new secret and generate an access token

Read a secret note

Read a secret using an access token

2. **Write/paste the secret note** you want to send. Select how long you want your secret note to remain stored. It will be kept until it been read. When finished, click **Store secret**.



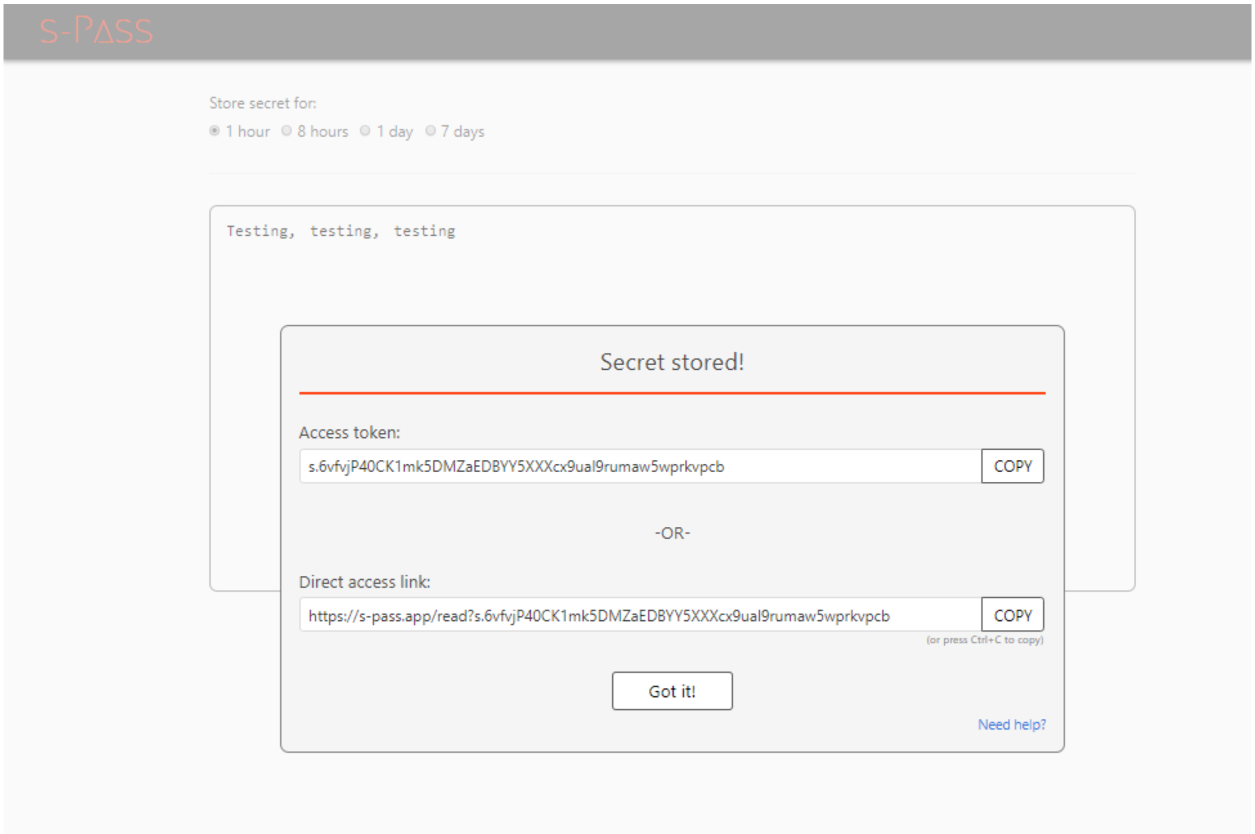
Store secret for:

● 1 hour ○ 8 hours ○ 1 day ○ 7 days

NOTE

Anyone with the token will be able to access your secret note during the time period you specified.

Your secret note is now stored**.** In the *Secret stored!* pop-up, copy the token OR copy the direct link to share your secret.



Store secret for:
● 1 hour ○ 8 hours ○ 1 day ○ 7 days

```
Testing, testing, testing
```

Secret stored!

Access token:
s.6vfvjP40CK1mk5DMZaEDBYY5XXXcx9ual9rumaw5wprkvpcb

-OR-

Direct access link:
https://s-pass.app/read?s.6vfvjP40CK1mk5DMZaEDBYY5XXXcx9ual9rumaw5wprkvpcb

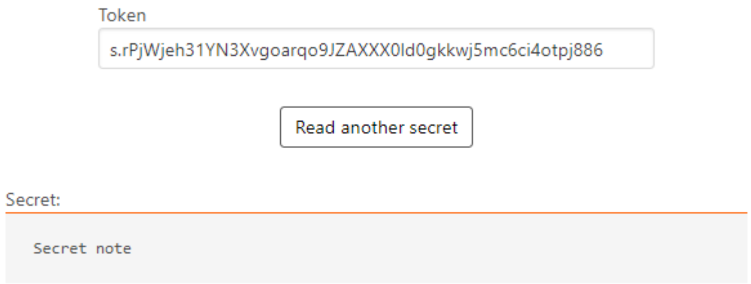
(or press Ctrl+C to copy)

NOTE

Your confidential information will be accessible only by the person who has the token or the link. Until viewed, the information is encrypted, unreadable to everyone and stored in the KDDI system.

Read a Secret

If you have a **direct access link,** paste it in a web browser and under the **Secret:** there is a gray box with the shared secret. If you have an **access token**, go to https://s-pass.app/, click **Read a secret note**, paste your token, and click **Submit token**.



Token
s.rPjWjeh31YN3Xvgoarqo9JZAXXX0ld0gkkwj5mc6ci4otpj886

Secret:

```
Secret note
```

NOTE

Once you read the secret note, it will be deleted from the system.

Secure File Transfer

Using the KDDI web interface, you can define methods for the transfer of Reports exports from KDDI towards the file transfer resources in your ownership. Methods enabled for this purpose are FTP and SFTP.

FTP is a file transfer protocol providing basic, unencrypted file transfer capability. Although it enables both anonymous access and authenticated sessions, the user credentials and data payload are transferred over public networks in cleartext, posing a **HIGH risk to unauthorized access to confidential data and the spreading of concealed malware.** Being completely replaced with more secure alternatives (SFTP, FTPS, SCP...), the FTP protocol should ONLY be used on extremely trusted and isolated systems or for public access anonymous FTP - none applicable to KDDI use cases.

We recommend using **SFTP (Secure FTP)**. All it takes is implementing an SFTP server on the client-side and providing access parameters, either via the KDDI web interface EXPORT feature or towards Customer Care.

Secure implementations usually include the following steps:

- Specifying a non-standard port (other than 22)
- Safelisting incoming (sender) IP addresses; when it comes to KDDI, these would be **193.105.74.4** and **62.140.31.104**
- Using dedicated credentials for EACH client user (i.e., credentials dedicated solely for KDDI)
- Choosing long, complex passwords (12 characters minimum)
- Changing passwords regularly (e.g., every three months)

Apart from security reasons, usage of the encrypted data transfers is - in many industries worldwide - **a regulatory compliance requirement** included in the security policy of businesses.

When you choose the insecure version of FTP, **you accept related security risks**, while KDDI renounces any liability possibly resulting from such use.

Client`s Internal Processes

Reinforce internal credentials storage and management to mitigate a potential risk of internal data leakage in the future which might result in unauthorized access to the KDDI platform and traffic costs.

For safekeeping of your passwords, consider using one of the commercial-grade password management tools.

Potential Risks if Controls Are Not Implemented

Credentials leak due to traffic interceptions when using unencrypted HTTP/SMPP traffic. This can happen in the following circumstances:

- When using unsecured HTTP combined with the basic authorization (username and password contained in the encoded form in the Authorization header) - which might have occurred on any node in between your network, ISPs and proxy services (if used), and the KDDI web interface.
- When applying MITM methods between the client network and the KDDI platform.
- In an insecure (plaintext) format in any kind of storage (digital and analog); KDDI stores users' passwords in a one-way hashed format with access privileges limited to only a few trusted employees; access is not granted to any 3rd party.
- In an insecure (plaintext) format during exchange/communications (via electronic channels, telephone, even live discussions).
- When you have not changed your password in a long time.