IS GENERAL APPENDIX

Applicable as from: 17 December 2018

RTE makes available to the User various Information System (IS) Applications that are adapted to the services to which the User has subscribed.

The 'Rules governing access to the RTE Information System and the use of RTE applications', known as the 'IS Rules', are available on the Customer Portal of RTE's Website and on the Services Portal of RTE.

This document is the IS General Appendix of the IS Rules. It lays down the general terms and conditions under which RTE IS Applications may be accessed and used:

- RTE IS Methods of Access; see § 4
- Accessible Applications and their Methods of Use; see § 6 and § 7
- User Equipment configurations supported by RTE to access the Applications; see § 8
- The Electronic Key user charter (*Particularly, the steps to be taken in the event of the loss of a key or a suspicion that a key is being used fraudulently*) - see § 10

The corresponding French document "Annexe SI Générale" (17 December 2018) shall prevail in the event of any differences in interpretation with this document.

CONTENTS

1 Introduction

To support the Services subscribed to by the User, RTE permits the latter to access, in a secure manner, its Information System (IS) and a number of Applications adapted to these Services.

The IS Rules specify the general terms and conditions under which the RTE IS may be accessed and the Applications may be used so that the Services can be provided. The IS Rules are an integral part of the contractual terms and conditions applicable to the services provided by RTE as part of its duties.

This IS General Appendix to the IS Rules lays down the general terms and conditions under which RTE IS Applications may be accessed and used. It provides a list of these Applications and sets out the technical terms and conditions under which RTE's IS and its Applications may be accessed.

Use of the IT resources provided by RTE is limited to the Applications for which a service contract between RTE and the User exists and the duration of the aforementioned contract.

Please note: The characteristics and the specific terms and conditions under which an Application may be used are specified in the Application's IS Application Appendix (Application User Guide, Message Implementation Guide, if applicable).

2 Terminology

The following terms, which are used in this appendix and whose first letter is a capital letter, are defined in the IS Rules:

- User;
- Method of Access;
- Access request;
- Application;
- Method of Use (of an Application);
- Electronic Key: Digital key, Logical Key;
- Holder (of an Electronic Key);
- Certification Policy;
- Software certificate;
- Message;
- Downgraded mode;
- Message Implementation Guide;
- Application User Guide.

3 Identification of the User: the EIC code

A standard exists to identify operators and to allow digital data to be exchanged efficiently within the European electricity market.

ENTSO-E (European Network of Transmission System Operators for Electricity) and ACER (Agency for the Cooperation of Energy Regulators) use a system to identify energy market operators: EIC codes (Energy Identification Code).

RTE has a local issuing office through which it issues EIC codes.

These codes allow operators, management areas and works to be identified: lines, production, demand-side management, and balancing entities, etc.

These codes are used by electricity market operators (grid operators, producers, balance responsible entities, etc.) for numerous data exchange operations.

When submitting an Access request as part of a service, the User must specify his EIC code, regardless of the issuing office allocated to him.

The party EIC code is compulsory to exchange data with RTE but it is not required to access the Customer Portal ('EPC'), metering data (dat@RTE), programming or the balancing mechanism (SyGA, e-Pat) – see § 7.

To obtain an EIC code, please use the form that can be found on the Customer Portal of RTE's Website ('To access to the market' section).

4 RTE IS Methods of Access

4.1 Access to RTE's Front Office

The RTE Front Office is all of the electronic media made available by RTE to allow access to its IS and the Applications.

Irrespective of the access method selected by the User, the telecommunications protocol used is Internet Protocol (IP). Unless stated otherwise, the ports used are the standard ports for the protocols indicated.

Any User who accesses RTE's Applications must be the Holder of a personal and non-transferable Electronic Key, which identifies and authenticates him.

This Electronic Key is issued to the User after an Access request has been made.

4.2 Access through the Internet

The RTE Front Office may be accessed through the Internet.

Applications may be accessed through the Internet using the domain names and addresses (URL) indicated in each Application's User Guide.

A User who accesses Applications through the Internet must be the Holder, depending on the Application, of a Logical Key: a soft Digital Key (software certificate) or a hard Digital Key (such as a chip card).

4.3 Other Methods of Access: 'Specialised Liaison'

RTE has entrusted the provision of network services to a Third Party to permit access to its Applications. These network services provide VPN access to the Applications. RTE's public sites cannot be accessed in this way.

Users are able to subscribe freely to these offers. These contracts may not incur the liability of RTE.

If requested, your customer relations manager will inform you about the services and Applications that may be accessed through these offers and direct you towards the Third Party responsible.

Two actors cannot share the same Specialised Liaison.

These other Methods of Access do not provide access to any additional functionality of the Applications. They do not rule out Internet-based access, which may also be requested. They are referred to as 'Specialised Liaison' methods in the rest of this appendix.

The main benefits of a Specialised Liaison are:

- a customised level of service;
- the automation of certain exchanges, particularly those of hosted messaging (explained later on), which are not possible with Internet-based access. As the User's login site is identified, RTE allows authorised Holders with a Specialised Liaison to log in to certain Applications with a Logical Key.

5 Software certificates: Withdrawal, Installation, Backup and Renewal

RTE issues Digital Keys in accordance with the Certification Policy published on the Customer Portal of its Website ('Request or change your IS access' section).

5.1 Withdrawal

When the Electronic Key is a Software certificate, the User receives an E-mail to withdraw the certificate from RTE's Certification Operator. The withdrawal process is a secure Internet-based operation. The E-mail specifies the actions to be performed and the User has 90 days to carry out these actions. RTE recommends that the withdrawal is performed as soon as possible. The certificate can be used 24 hours after it has been withdrawn, at the latest.

If the User does not withdraw his Software certificate within 90 days, the certificate is automatically revoked by RTE. The User will then have to submit another Access request form.

5.2 Installation

The withdrawal process includes the installation of the Software certificate in the certificate file on the User's workstation. This requires rights that may not have been granted, in compliance with the User's security policy, to the account used on the workstation (e.g.: Windows account).

If access is requested for the first time for a Holder, RTE recommends that the User's IT department provide assistance during the installation of the Software certificate issued by RTE.

5.3 Backup

RTE recommends that the Holder of a Software certificate save it in a lasting and secure manner. This recommendation also applies to the passwords that will allow it to be reinstalled in the event his workstation is changed or breaks down.

5.4 Validity period and Renewal

A Software certificate is valid for a limited period: three years. The validity period begins on the day the User withdraws the certificate. The expiry date is shown on the Certificate.

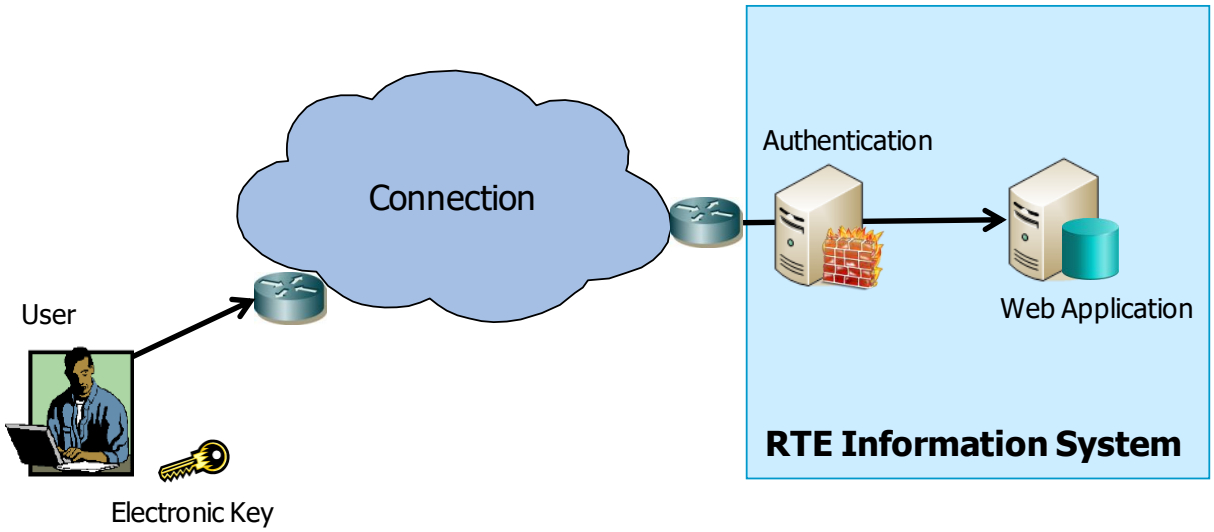
Unless requested otherwise, a Software certificate is tacitly renewed and the User receives an E-mail with which he can withdraw a new certificate 40 days before the expiry date.

In order to avoid any interruption to the User's access to the Applications, RTE recommends that the User withdraw the certificate as soon as possible.

6 Methods of Use of the Applications

6.1 'Web' Method of Use

6.1.1 Manual Access



This Method of Use allows any User with access to RTE's IS to log in to the Application from an individual workstation through a browser (pages shown in HTML format).

The User authenticates himself with the Electronic Key issued by RTE.

Characteristics of Web access

GRT (Guaranteed recovery time)	That of Third Parties providing connection equipment and telecommunication resources
Methods of Access	Internet or Specialised Liaison
Security	Authentication: • Internet access: Digital or Logical Key depending on the Application • Specialised Liaison: Digital or Logical Key depending on the Application Confidentiality: Use of the TLS protocol to encrypt exchanges between the User's workstation and the Application.
Installation	Simple
Implementation	Fast
Bandwidth	Depends on the Third Parties providing connection equipment and telecommunication resources between the User's workstation and RTE's Front Office
Protocol	HTTPS (Hypertext Transfer Protocol Secure)

6.1.2 Uploading of documents in HTTPS

For certain services, the User must send RTE files whose format is predefined and the protocol is a HTTP upload.

The User must first establish a secure connection (HTTPS) to the URL indicated by RTE for the service.

RTE expects the data to be sent in a 'multipart post' HTTP request, namely, inserted in the 'post' request as attached files (RFC 1521 – MIME).

In this case, the term, 'file', refers to an electronic document that does not have to be turned into a file when it is sent or received.

Such an exchange is simply automatable. When the exchange is infrequent and for 'backup mode' type situations, RTE also provides a Web interface so that it can be performed manually.

6.2 'Messaging' Method of Use

For certain services, the User may or must send Messages attached to E-mails sent to the mailbox of an RTE Application.

The Application replies through an Acknowledgment of technical reception ('ART') or a Functional acknowledgment of receipt ('ARF'). Certain Applications also publish data by sending Messages attached to E-mails sent to the User's mailbox.

A messaging service, associated with the name of the domain @services.rte-france.com[1], exchanges the E-mails.

The messaging service has two Methods of Use: Hosted messaging and Encrypted messaging. Certain services combine Web access to an Application and messaging exchanges (see § 7).

The main characteristics of these two Methods of Use are:

Characteristic	Hosted messaging	Encrypted messaging
E-mail address	RTE gives the User a domain address (@services.rte-france.com). A Holder appointed by the User is given responsibility for the mailbox.	The E-mail address is provided by the User (e.g.: @societe.com) and is associated with a Holder.
Temporary storage of E-mails sent by RTE and not withdrawn by the User	On the messaging server of RTE's Front Office.	On a messaging server belonging to the User or to the hoster chosen by the User.
E-mail Routing Method	Through a temporary connection (VPN tunnel[2]) between the User's workstation and the messaging server of RTE's Front Office.	The E-mail goes to the sender's mail relay, which then routes the E-mail through the Internet to the recipient's messaging server.
Security	The User authenticates himself with the Digital Key issued by RTE to open and temporarily establish the tunnel. E-mails exchanged in the tunnel are encrypted automatically.	The E-mails are signed and encrypted with Digital Keys (Software certificates) issued by RTE before being routed through the Internet.

1 The 'historical' domain, @400kv-services.rte-france.com, also exists.

2 VPN = Virtual Private Network

6.2.1 Hosted messaging

Allocation of a mailbox to a User

Under this Method of Use, a mailbox on the Front Office messaging server (known as a 'hosted mailbox') is allocated to the User as part of a service and of an Application. The E-mail address therefore has an equivalent composition:

<EIC Code><Application>@services.rte-france.com

where <EIC Code> is that of the User and where <Application> is the code of the RTE Application or service for which the hosted mailbox is used (see § 7).

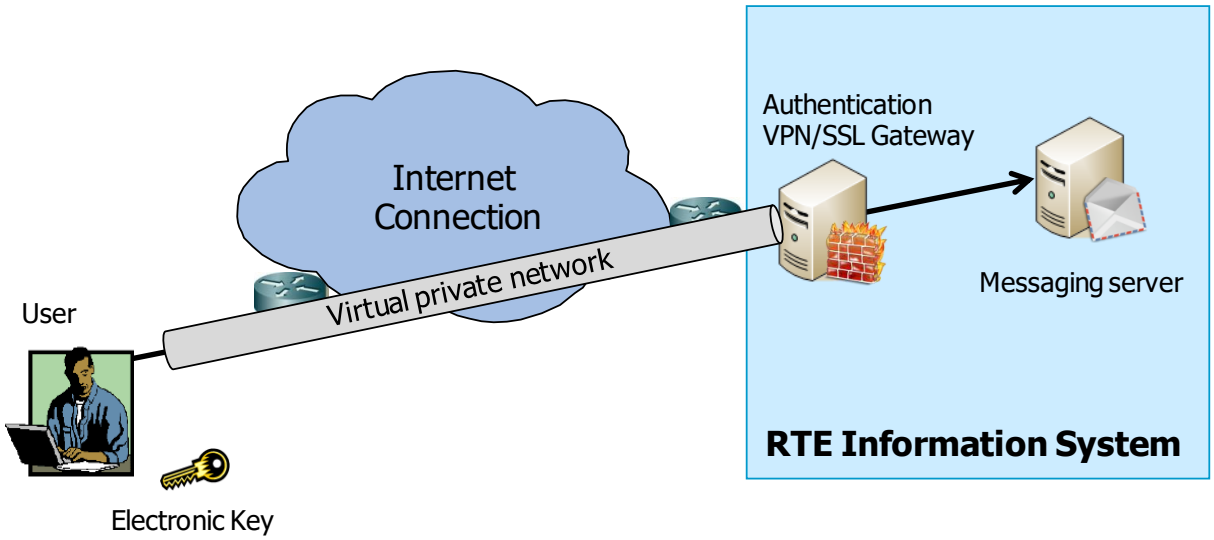
Any exchange performed by a hosted mailbox is considered to have been carried out on behalf of the User.

The hosted mailbox is associated with a Holder appointed by the User in the Access request form. The messaging service's connection settings (E-mail address, identifier, and password) are sent to the Holder in a secure manner.

To appoint another Holder, the User must submit an Access request form.

User access to the hosted messaging service through the Internet

When the User accesses RTE's IS through the Internet, the hosted mailbox can only be accessed after the User has temporarily established a virtual private network (a VPN tunnel) between his workstation and a piece of equipment in RTE's Front Office; this is known as a 'VPN/SSL Gateway[3]'.



To establish the virtual private network, the User enters an Internet address (an URL), provided by RTE, into his browser and identifies himself and authenticates himself with the Digital Key issued by RTE.

The purpose of the virtual private network is to ensure the confidentiality of all exchanges by encrypting all transmitted data automatically.

[3] SSL is a standard protocol used to secure Internet-based exchanges. New versions of the protocol are called TLS.

When logging in to the VPN/SSL Gateway for the first time, client software is downloaded and installed automatically on the User's workstation, which must be a Windows workstation. This operation requires 'administrator' rights. This program is used to establish the private virtual network and to direct only SMTP and POP connections intended for RTE's messaging service to this virtual network (see below).

Using Hosted messaging

The SMTP protocol (Simple Mail Transfer Protocol) must be used to send an E-mail to the mailbox of an Application. The POP protocol (Post Office Protocol) must be used to read the E-mails received from RTE in the hosted mailbox. E-mails cannot be sent, read or handled directly from a browser through a Webmail interface.

To carry out these exchanges, the User must run on his workstation a messaging client software (see § 8), which is either installed or portable. This software must be configured, on the one hand, with the SMTP and POP servers of the Front Office messaging service whose domain names are provided by RTE and, on the other, with the settings to access the hosted mailbox.

The hosted mailbox may only be used for work-related exchanges between the User and RTE, as stated in the service contracts and in accordance with the IS Application Appendices (Application User Guide, Application Message Implementation Guide). The mailbox may therefore be consulted by RTE. No mail can be sent to a non RTE managed domain, for it is rejected. RTE managed domains currently are: rte-france.com, 400kv-services.rte-france.com, services.rte-france.com.

A hosted mailbox is a place where E-mails are exchanged and a place that allows E-mails sent by RTE to be stored temporarily. A quota management system is used to restrict its size.

The amount of space allocated by default is 20 MB. It may be increased on request to no more than three months of data.

Detailed characteristics of Hosted messaging

GRT (Guaranteed recovery time)	That of Third Parties providing connection equipment and telecommunication resources
Methods of Access	Internet or Specialised Liaison
Security	Authentication to establish a communication channel: • Internet: Digital key, authentication of the key holder. • Specialised Liaison: Authentication of the User's site when the connection is established. Authentication for exchanges with the messaging server using the identifier, password Confidentiality: • Internet: TLS protocol encryption • Specialised Liaison: encryption of the Specialised Liaison.

Installation	Internet access: When logging in to the VPN/SSL Gateway for the first time, client software is downloaded and installed automatically on the User's workstation. All Modes of Access: access to the messaging service requires a standard messaging client software (see § 8.1)
Implementation	Fast
Bandwidth	Depends on the Third Parties that provide connection equipment and telecommunication resources
Protocol	HTTPS (Hypertext Transfer Protocol Secure) to establish the VPN/SSL tunnel (Internet Access) SMTP (Simple Mail Transfer Protocol) to send E-mails POP (Post Office Protocol) to withdraw E-mails
Format of the E-mails	MIME (Multipurpose Internet Mail Extensions) - Standard Internet defined by the IETF (Internet Engineering Task Force)
Routing guarantee	The User can see immediately if E-mails can or cannot be sent or withdrawn on RTE's messaging server, regardless of the cause (the User's own IS, the telecommunication network, RTE's IS). The User can then decide on the corrective measures to be taken or place the service in downgraded mode.

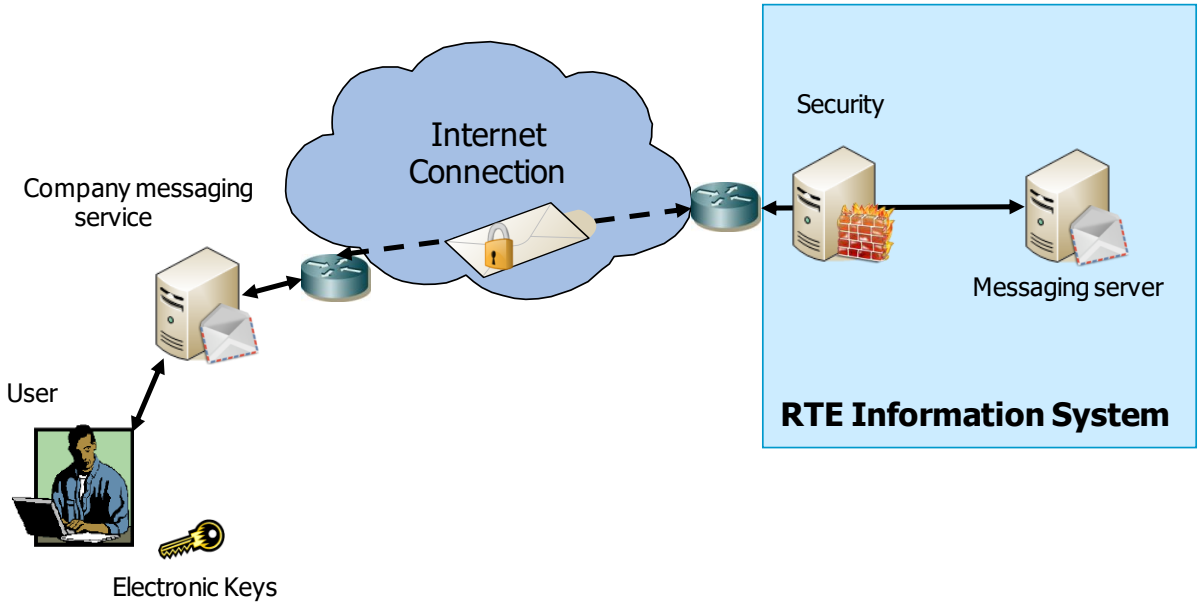
6.2.2 Encrypted messaging

The E-mail address is provided by the User in the Access request form.

Exchanged E-mails must be signed and then encrypted with Software certificates issued by RTE. The E-mails are sent and received by the Front Office using the SMTP protocol and their format must be S/MIME.

Any exchange performed with the mailbox is considered to have been carried out on behalf of and under the responsibility of the User.

To carry out these exchanges, the User must run a messaging client software on his workstation (see § 8).



Detailed characteristics of Encrypted messaging

GRT (Guaranteed recovery time)	That of Third Parties providing connection equipment and telecommunication resources
Method of Access	Only the Internet
Security	The User authenticates himself by signing the E-mail with his Software certificate (*private key*). The E-mail, encrypted with the Software certificate of the recipient Application (*public key*), can only be read by RTE. In turn, E-mails from the Application to the User are signed by RTE and encrypted with the Software certificate (*public key*) associated with the User's E-mail address.
Installation	E-mails are sent using a standard messaging client software (see § 8.1). 'Administrator' rights are required to install certificates in the messaging client software certificate keystore.
Implementation	To exchange E-mails signed and encrypted with an RTE Application, three certificates must be installed in the workstation's messaging client software certificate keystore. These are: • the Software certificate (*private key and public key*) associated with the User's E-mail address, a certificate issued by RTE. • The Software certificate (*public key*) associated with the RTE Application E-mail address; • The Software certificate (*public key*) of the RTE Certification Authority ('AC'), used to issue RTE certificates. Implementation may also require actions that fall outside of the area of expertise of the Certificate holders and of RTE's technical department. For example: • Certain messaging servers incorrectly consider encrypted/signed E-mails to be spams. • The legal notice that is sometimes added to the end of an E-mail causes the E-mail to be rejected when it is received by RTE. The integrity analysis considers the E-mail received not to be the one signed by the sender as its content was altered after it was signed.
Bandwidth	Depends on the Third Parties that provide connection equipment and telecommunication resources
Protocol	The SMTP protocol (Simple Mail Transfer Protocol) for the sending of E-mails. Note: RTE's IS is not responsible for the withdrawal of E-mails. This operation constitutes an exchange between the User's workstation and his messaging server.
Format of the E-mails	S/MIME (Secure / Multipurpose Internet Mail Extensions) - Standard Internet defined by the IETF
Routing guarantee	The successful transmission of an E-mail by the User to his mail relay does not mean that the E-mail has been received by RTE's messaging server.

7 List of Applications and their Methods of Use

Service or Application	Customers or Suppliers concerned*	Brief description	Methods of use
EPC	Electricity market operators	RTE Customer Services Portal – see EPC Guide	Web Application
Dat@RTE (Provision of your data. E.g. meter readings, forecast position)	CO, IP, DSO	'Transmission System Access' basic service	Web Application
		'Transmission System Access Data' Dat@RTE service offer, option 1 or option 2	Encrypted messaging
	DSO	'Reconstitution of PDN (Public Distribution Network) flows' basic service	Encrypted messaging
	BRE	'BRE' basic service 'BRE data' Dat@RTE service offer 'Forecast position' Dat@RTE service offer	Web Application Hosted messaging
PEB	BRE	Block Exchange Program (NEB replaced by PEB since 1 September 2018)	Web Application
ENVOI-NEB-SITES-RPD	DSO	Sending by RTE to the DSO of exchanged blocks ('NEB') with sites from its Public distribution network (PDN)	Encrypted messaging
NER	RRE	Reserve Exchange Notification	Hosted messaging
NEBEF	DSMO	Load reduction programming	Hosted messaging
		Consumption curves of sites that are load-reducible and not read remotely	Poste restante
	BRE	Total load reduction retained in the area of the BRE	Hosted messaging
	DSO	Total load reduction retained on the distribution network. Consumption curves of sites that are load-reducible, read remotely and connected to the transmission networks	Encrypted messaging
DSO referential	DSO	Reference data exchange interface	Encrypted messaging
DIAPASON	DSO	Dynamic data exchange interface	Encrypted messaging
SyGA	BA	Participation in the Balancing Mechanism Sending and management of balancing offers	Web Application
	PRE	Intraday redeclarations of schedules (programmes)	Web Application
e-PAT	PRE	Sending of schedules (Call programmes) to RTE in the form of three values	Web Application Hosted messaging
TAO	BA	Automated transmission of Balancing Orders	Web Application
CRMA (Verification of Balancing Orders)	DSO	Consumption / production curves of the balancing entities connected to the distribution networks	Encrypted messaging
	BA	Consumption curves of sites that can take part in diffuse balancing.	Uploading of files in HTTPS or 'Poste restante'
MORGAN	IA	Capacity allocation and Nomination of energy exchanges on international interconnectors.	Web Application (Hosted messaging is optional)
Transparency	Prod, CO	Sending of production and consumption data to RTE (e.g.: Forecast, Actual, Unplanned outage)	Uploading of files in HTTPS
e-losses	LS	Consultation of RTE for the provision of energy for losses over several months up to several years	Web Application
AP / FAP	LS	Sending by RTE of the Daily schedule and monthly billing of loss purchases.	Hosted messaging

Service or Application	Customers or Suppliers concerned*	Brief description	Methods of use
EEB **ODALI**	Engineering and construction companies	Entry of materials required to undertake works associated with electrical facilities so that they can be supplied. Communication with RTE's Logistics unit regarding matters related to Industrial Logistics flows.	Web Application
e-appro	Suppliers	RTE orders as part of general and 'IT-PI' (IT - Telecommunications - Intellectual Services) purchases	Web Application

* The types of Customer/Supplier are:

BA..... Balancing Actor
IA ..... Interconnections Actor
CO ..... Consumer
LS ..... Losses Supplier (RTE energy supplier for losses)
DSO ..... Distribution System Operator
DSMO..... Demand-side Management Operator
IP..... Independent Producer
Prod ..... Producer
BRE..... Balance Responsible Entity
PRE..... Programming Responsible Entity
RRE..... Reserves Responsible Entity

Remarks:

- This table is provided for information purposes only. The characteristics of an Application or service and the terms and conditions under which the aforementioned may be used are laid down in the corresponding 'IS Application Appendix' (User Guide, Message Implementation Guide, if applicable).
- A User who exchanges data in 'Encrypted messaging' mode with an Application for which this Method of Use is no longer offered may continue to use this method.
- RTE will never receive E-mails uploaded using the 'Hosted messaging' mode if the destination Application requires the use of the 'Encrypted messaging' mode.

8 User Equipment configurations supported by RTE to provide access to its Applications

'Equipment' is understood to mean any hardware or software, whether owned or not by the User, used to access the telecommunications network, RTE IS Applications or RTE's Front-Office messaging service.

This section specifies the configurations supported to access RTE Front-Office services on the basis of three criteria:

- Operating systems supported.
- Browsers supported to access the Web Applications and hosted messaging through VPN/SSL.
- Messaging client software supported.

A 'supported' configuration is a configuration that is currently supported by the editor and included in the following tables. RTE commits itself to ensuring that access functions or to providing a workaround or a solution as quickly as possible when the issue comes from RTE's infrastructure for such as configuration.

The user manuals for the configurations supported are published on the Customer Portal of RTE's Website ('Obtain access' section).

RTE does not guarantee access to its Applications from any other configuration. Particularly, automated tools (scripts, packages, specific developments, etc.) are not supported.

8.1 Operating systems supported

Operating system Editor	Version
Microsoft Windows	7, 8.1, 10

8.2 Browsers supported

Browser Editor	Windows 7, 8.1, 10
Microsoft Internet Explorer	11
Mozilla Firefox	> 45 (ESR)

8.3 Messaging client software supported

Messaging client software Editor	Windows 7, 8.1, 10
Microsoft Outlook	2013
Mozilla Thunderbird	> 45 (ESR)
Lotus Notes	9

9 RTE Application access request

To obtain access to RTE Applications adapted to the services to which the User has subscribed, the User must submit an Access request by completing an electronic or paper-based form and sending it to RTE.

This form can be found on the Customer Portal of RTE's Website ('Request or change your IS access' ' section) and on the Services Portal of RTE.

An Access request is required for each physical person who has to access and use RTE Applications. Each person becomes the Holder of the Electronic Key that is issued to the person in question.

10 The Electronic Key user charter

An Electronic Key is issued so that you can access the IS and use RTE's Applications. It lets you authenticate yourself and ensure that your exchanges with RTE's IS and Applications remain confidential.

The Electronic Key is strictly personal and non-transferable. You are entirely responsible for using and safeguarding it. Consequently, access to RTE's IS and use of an RTE Application thanks to an Electronic Key are considered to have been carried out by the User.

By accepting this Electronic Key, you agree to take all measures necessary to ensure that it is not divulged to or used by a Third Party.

If this Electronic Key is digital and on a chip card, it is sent to you by post. The key's PIN code is sent in a separate letter. Memorize the code and do not write it down on anything that could be taken from you at the same time as the chip card.

In the event the Electronic Key is **lost** or if you believe that it could have been **used fraudulently**, you must immediately call the **RTE Hotline** on **00 800 80 50 50 50** (international freephone number) or **0810 80 50 50** (shared-cost number) to ask for the Key to be **revoked**.

During the revocation process, you will have to provide the '**Password selected**' (previously '*PKI Holder Authenticator*' or '*Personal Authenticator*') entered in the Access request (made through a paper-based or electronic form).

As a precautionary measure, RTE may ask you to change your Electronic Key.

Finally, before accessing RTE's Applications, please consult:

- On one hand, the 'Rules governing access to the RTE Information System and the use of RTE applications' and the 'IS General Appendix', which lay down the general terms and conditions under which the IS may be accessed and the Applications may be used for the execution of the service.
- On the other, the 'RTE France' Certification Authority's Certification Policy, which contains all of the rules and obligations governing the use of Digital Keys.

These documents are published on the Customer Portal of RTE's Website and on the Services Portal of RTE.

RTE would like to inform you that certain personal data is kept in a paper-based and/or electronic format for the security requirements specified in the aforementioned documents.

Under the French **data privacy** law of 6 January 1978, you have the right to access, amend and delete information that concerns you. To exercise this right, speak to your RTE contact.

~°~°~°~°~°~°~°~°~° End of document ~°~°~°~°~°~°~°~°~°~°~°