Le réseau de transport d'électricité

CERTIFICATE FOR ACCESS TO RTE APPLICATIONS (PKI)

Organisation and changes to the renewal process - November 2022

Presentation of the main principles

The role of PKI

Public Key Infrastructure (PKI) is used to meet the security needs for data exchange with our customers. PKI provides user authentication, confidentiality and data integrity functions.

All RTE applications require a certificate for authentication use and authorisation to allow access.

Two types of certificates are now available to customers:

- **Software Certificates (most common)**
- Hardware certificates (this is a chip card to be installed by the customer, only for the E-Losses application)

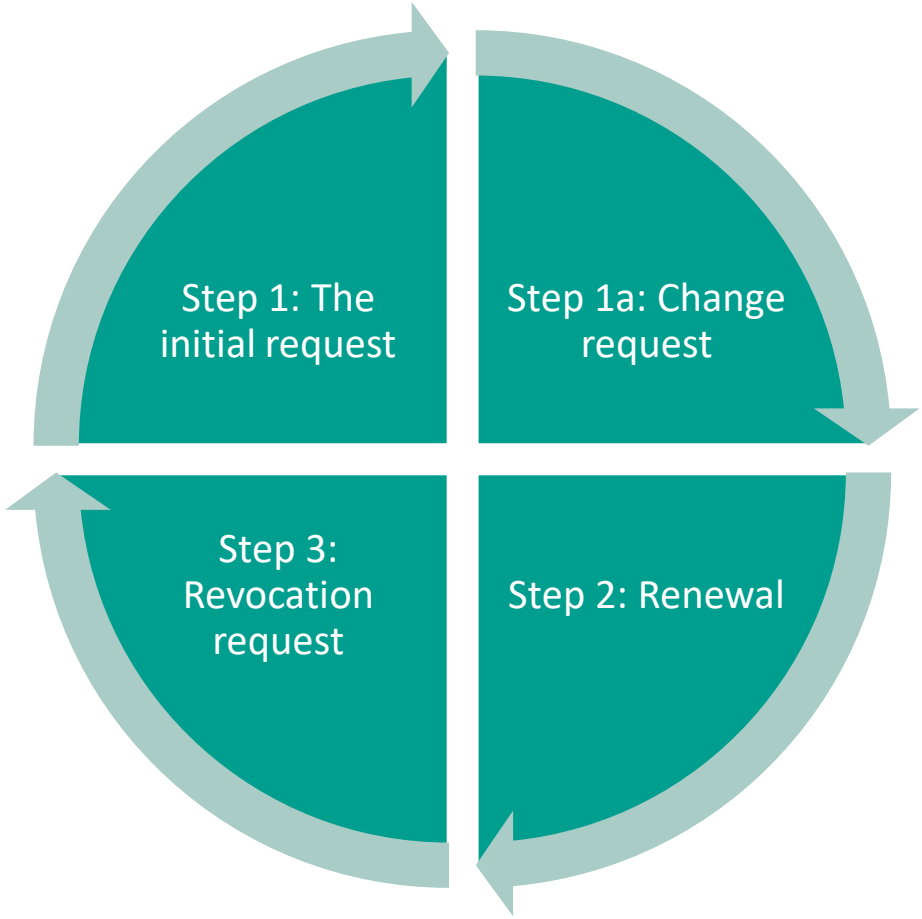
Principles

1 user (email address of the holder) = 1 company perimeter = n authorisations to RTE applications = 1 certificate

It is possible to provide a different contact email address from the email address of the holder, particularly for receiving communications relating to the life cycle of the certificate.

NB: The rest of the presentation addresses only software type certificates

The life cycle of a certificate



Life cycle of a certificate

Step 1: The initial request

Submitting a request on the Service Portal

1

- All requests must be made from the "*Demander un certificat (PKI)* (Request a Certificate (PKI))" request form available at the bottom of the Service Portal.
- The form is pre-filled with the requester's profile information (prerequisite: the requester must have a private account on the Portal).
- The applications are pre-selected according to the type of customer (generator, consumer, distributor, market player).
- The request can be made for requesters themselves, for a bot access (machine-to-machine) or for any user in the company who is an administrator.

Processing of the request by RTE

2

- Validation of the form generates a summary document in PDF format. This document is sent to the requester, administrators and RTE for processing.
- RTE creates the certificate and sends it within 24 business hours.
- Application authorisations are also taken into account within 24 hours, except when additional information is required.

Certificate generation and installation

3

- The requester receives a certificate retrieval email.
- Using the link, the requester enters their email address, authenticator (which they provided on their initial request on the Service Portal form) and retrieval code (provided in the retrieval email), then downloads their certificate and installs it on their computer.
- **The certificate has a lifespan of 3 years from the date of retrieval by the applicant.**
- **The applicant can now access RTE applications.**

Life cycle of a certificate

Step 1a: Change request

Making a change request

1

- It is possible to request additional access (e.g. access to an application recently deployed by RTE). In this case **it is absolutely not necessary to reapply for a certificate**. Simply request additional authorisation from the hotline.

- In addition to their email address, certificate holders can request to add an additional contact email address. This request can also be made via the hotline.

Life cycle of a certificate

Step 2: Renewal -

Automatic renewal (until 15 January 2023)

1

- The current policy is that all certificates must be automatically renewed. **This is done 40 days before the expiry date.**
- The renewal action triggers an email in the same way as for a certificate creation but the current certificate of the user remains functional (until the expiry date or until the retrieval of the new certificate). The email is sent from the electronic mailbox RTE-adminCertificat@idnomic.com by the hotline.
- The email is sent to the holder of the certificate and to the contact email address.

Certificate generation and installation

2

- RTE proceeds with the renewal.
- The user receives an email allowing retrieval and installation of their new certificate. The email is sent by the hotline from the electronic mailbox RTE-adminCertificat@idnomic.com.
- The user installs the certificate in the same manner as the initial installation. The previous certificate is deactivated automatically when the new one is installed.

Life cycle of a certificate

Change in the certificate renewal process

- RTE is in the process of changing the certificate renewal policy, **which will now be triggered following an explicit request from the holder.**

- In particular, the new process should make it possible to:
  - Secure the chain,
  - Limit the number of certificates in circulation,
  - Give administrators visibility regarding access requests but also requests to renew access to RTE applications made by their employees.

Life cycle of a certificate

Step 2: Renewal -

Renewal at the initiative of the user (from 16 January 2023)

1

- **The user is informed by email 40 days before the expiry of the certificate and is invited to make a renewal request. The request must be made as soon as possible and no later than 5 business days before the expiry date in order to ensure continuity of access to the services.**
- The user makes the request on the Service Portal via the form "Renew or delete a certificate (PKI)". The administrator can submit a renewal request for any user within its company.
- A summary of the renewal request is sent to the user, administrator and RTE.

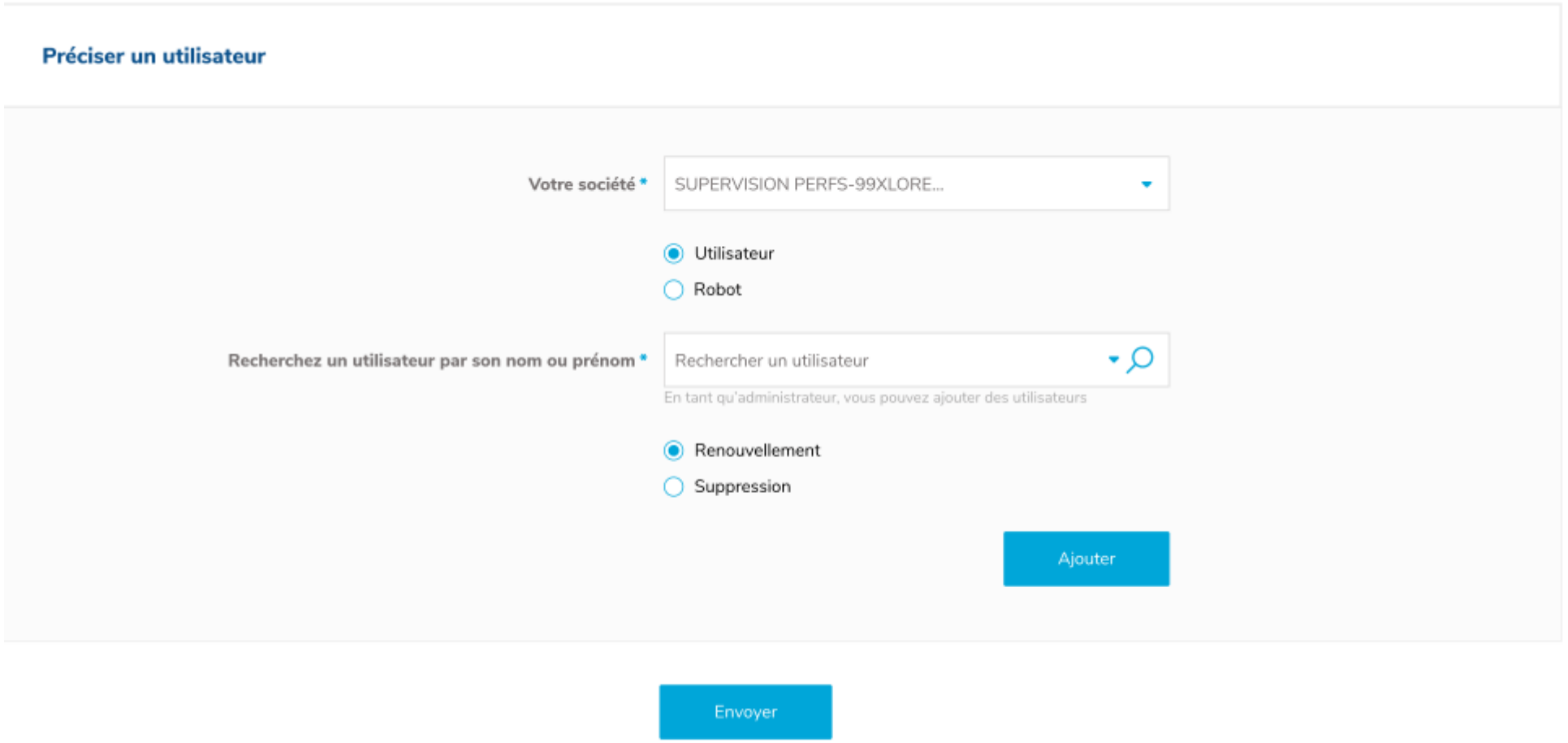
Certificate generation and installation

2

- RTE proceeds with the renewal.
- The user receives an email allowing retrieval and installation of their new certificate. The email in question is sent from the electronic mailbox RTE-adminCertificat@idnomic.com by the hotline.
- The user installs the certificate in the same manner as the initial installation. The previous certificate is deactivated automatically when the new one is installed

Life cycle of a certificate

Step 2: Renewal
-



Life cycle of a certificate

Revocation

1

- If the user has not retrieved their certificate following receipt of the email, the certificate is deleted from the tools, making it unusable. RTE must respect a period of 90 days before revoking.
- Customers will not receive any email following this action and will need to make an initial request if they still wish to have access to RTE applications.

Deletion request

2

- The user can submit a deletion request by using the form available on the Service Portal. The administrator can submit a deletion request for any user within its company.
- The deletion request is processed by RTE within 24 business hours.

A few tips…

Access:

- The prerequisite to make a request for access to RTE applications for a company perimeter is **to have a private account on the Service Portal**. This prerequisite for the renewal request will be valid soon. As an administrator, we advise you **to plan ahead and create an account for all of your employees** who require access to an RTE application.

The initial request:

- The summary PDF of the request is sent immediately after validation of the form. **Please remember to check your spam folder** if you do not see anything in your main inbox (recipient address: no-reply@rte-france.com).
- The email allowing you to retrieve your PKI certificate will be sent to you within 24 business hours. **Please remember to check your spam folder** also (recipient's address: RTE-adminCertificat@idnomic.com).

Renewal:

- The email allowing you to retrieve the new certificate is sent from the same mailbox as the initial request and contains exactly the same information. To retrieve the certificate, you will be asked to enter the password you set on your initial request. **If you have forgotten your password you can submit a request to with the hotline to reset it.**

Deletion:

- As an administrator of the Service Portal, you can make deletion requests for any employee in your company. **If you would like a list of all PKI certificates for your company's scope, you can contact your account manager**.