DECISÃO n.º 2/2020 DO COMITÉ MISTO CRIADO PELO ACORDO ENTRE A UNIÃO EUROPEIA E A CONFEDERAÇÃO SUÍÇA SOBRE A LIGAÇÃO DOS RESPETIVOS REGIMES DE COMÉRCIO DE LICENÇAS DE EMISSÃO DE GASES COM EFEITO DE ESTUFA

de 5 de novembro de 2020

relativa à alteração dos anexos I e II do Acordo e à adoção de normas técnicas de ligação (NTL) [2021/1034]

O COMITÉ MISTO,

Tendo em conta o Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa ([1]) («Acordo»), nomeadamente o artigo 3.º, n.º 7, e o artigo 13.º, n.º 2,

Considerando o seguinte:

(1) A Decisão n.º 2/2019 do Comité Misto ([2]) alterou os anexos I e II do Acordo, satisfazendo assim as condições para o estabelecimento da ligação previstas no Acordo.

(2) Na sequência da adoção da Decisão n.º 2/2019 do Comité Misto e nos termos do artigo 21.º, n.º 3, do Acordo, as Partes trocaram os seus instrumentos de ratificação ou aprovação, pois entendem estar satisfeitas todas as condições para o estabelecimento da ligação previstas no Acordo.

(3) Nos termos do artigo 21.º, n.º 4, do Acordo, este entrou em vigor em 1 de janeiro de 2020.

(4) O anexo I do Acordo deve ser alterado nos termos do artigo 13.º, n.º 2, do Acordo a fim de assegurar uma transição harmoniosa na gestão dos operadores de aeronaves atribuídos à Suíça pela primeira vez, tendo em conta os progressos realizados no estabelecimento da ligação entre registos.

(5) Para ter em conta os desenvolvimentos recentes e garantir um maior nível de flexibilidade no estabelecimento da ligação entre registos exigida pelo Acordo, o anexo II do Acordo deve ser alterado nos termos do artigo 13.º, n.º 2, do Acordo, com vista a prever um conjunto de tecnologias alargado, mas equivalente, que permita criar essa ligação.

(6) Em conformidade com o artigo 3.º, n.º 7, do Acordo, o administrador do Registo Suíço e o administrador central do Registo da União elaboram normas técnicas de ligação (NTL) que tenham por base os princípios enunciados no anexo II do Acordo. As NTL devem incluir uma descrição pormenorizada dos requisitos relativos ao estabelecimento de uma conexão sólida e segura entre o Diário de Operações Complementares da Suíça (DOCS) e o Diário de Operações da União Europeia (DOUE). As NTL devem produzir efeitos logo que a decisão do Comité Misto seja adotada.

(7) Conforme disposto no artigo 13.º, n.º 1, do Acordo, o Comité Misto deve acordar orientações técnicas para assegurar a correta aplicação do Acordo, incluindo em relação ao estabelecimento de uma conexão sólida e segura entre o DOCS e o DOUE. As orientações técnicas podem ser elaboradas por um grupo de trabalho criado nos termos do artigo 12.º, n.º 5, do Acordo. O grupo de trabalho deve incluir, pelo menos, o administrador do Registo Suíço e o administrador central do Registo da União, devendo prestar assistência ao Comité Misto no exercício das suas funções nos termos do disposto no artigo 13.º do Acordo.

(8) Dada a natureza técnica das orientações e a necessidade de as adaptar à evolução em curso, as orientações técnicas elaboradas pelo administrador do Registo Suíço e pelo administrador central do Registo da União devem ser apresentadas ao Comité Misto para informação ou, se for caso disso, para aprovação,

([1]) JO L 322 de 7.12.2017, p. 3.

([2]) Decisão n.º 2/2019 do Comité Misto, de 5 de dezembro de 2019 criado pelo Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa, de 5 de dezembro de 2019, que altera os anexos I e II do Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa (JO L 314 de 29.9.2020, p. 68).

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

O anexo I, parte B, ponto 17, segundo parágrafo, do Acordo passa a ter a seguinte redação:

«Os operadores de aeronaves atribuídos à Suíça pela primeira vez após a entrada em vigor do presente acordo passam a ser da responsabilidade da Suíça depois de 30 de abril do ano em que é feita a atribuição e assim que a ligação provisória entre registos estiver operacional.»

Artigo 2.º

O anexo II, quarto parágrafo, do Acordo passa a ter a seguinte redação:

«As NTL especificam que as comunicações entre o DOCS e o DOUE consistem em trocas seguras de mensagens de serviços Web baseados nas seguintes tecnologias (*) ou em tecnologias equivalentes:

— serviços Web que utilizam o Protocolo Simples de Acesso a Objetos (SOAP),

— redes privadas virtuais (RPV) baseadas em equipamento informático,

— XML (Linguagem de Marcação Extensível),

— assinatura digital e

— protocolos de sincronização de tempo (NTP).

(*) Estas tecnologias são atualmente utilizadas para estabelecer uma ligação entre o Registo da União e o Diário Internacional de Operações, assim como entre o Registo Suíço e o Diário Internacional de Operações.»

Artigo 3.º

São adotadas as normas técnicas de ligação (NTL) apensas à presente decisão.

Artigo 4.º

É criado um grupo de trabalho nos termos do artigo 12.º, n.º 5, do Acordo, que prestará assistência ao Comité Misto para assegurar a correta aplicação do mesmo, incluindo no que se refere à elaboração de orientações técnicas para a aplicação das NTL.

O grupo de trabalho incluirá, pelo menos, o administrador do Registo Suíço e o administrador central do Registo da União.

Artigo 5.º

A presente decisão entra em vigor no dia da sua adoção.

Feito em Bruxelas, em 5 de novembro de 2020.

Pelo Comité Misto	A Presidente	Secretária da Suíça
Secretária da União Europeia	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

ANEXO

Normas Técnicas de ligação (NTL) nos termos do artigo 3.º, n.º 7, do Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa

NORMAS PARA A SOLUÇÃO PROVISÓRIA

1. **Glossário**

Quadro 1-1

Acrónimos relativos à atividade comercial e definições

Acrónimo/Termo	Definição
Licença	Uma licença para emitir uma tonelada de equivalente de dióxido de carbono durante um determinado período, válida apenas para efeitos de cumprimento dos requisitos do CELE [anteriormente designado por «RCLE-UE»] ou do RCLE da Suíça.
CH	Confederação Suíça.
CHU	Licenças de emissão gerais da Suíça (o termo «CHU2» é utilizado como abreviatura de licenças CHU para o segundo período de compromisso).
CHUA	Licença de emissão da aviação da Suíça.
POC	Procedimentos Operacionais Comuns desenvolvidos conjuntamente pelas Partes no Acordo com vista a operacionalizar a ligação entre o CELE e o RCLE da Suíça.
RegCLE	Registo de comércio de licenças de emissão.
RCLE	Sistema de comércio de licenças de emissão.
UE	União Europeia.
LUE	Licença de emissão geral da UE.
LUEa	Licença de emissão da aviação da UE.
RCUE	Registo Consolidado da União Europeia.
DOUE	Diário de Operações da União Europeia.
Registo	Um sistema contabilístico para as licenças emitidas ao abrigo do RCLE, que mantém um registo da propriedade das licenças depositadas em contas eletrónicas.
DOCS	Diário de Operações Complementares da Suíça.
Operação	Um processo inscrito num registo, que inclui a transferência de uma licença de uma conta para outra.
Sistema de diário de operações	O diário de operações contém um registo de cada operação proposta enviada de um registo para o outro.

Quadro 1-2

Acrónimos técnicos e definições

Acrónimo	Definição
Criptografia assimétrica	Utiliza chaves públicas e privadas para cifrar e decifrar dados.
Autoridade de Certificação (AC)	Entidade que emite certificados digitais.

Acrónimo	Definição
Chave criptográfica	Um elemento de informação que determina o resultado funcional de um algoritmo criptográfico.
Decifragem	Processo inverso à cifragem.
Assinatura digital	Uma técnica matemática utilizada para validar a autenticidade e integridade de uma mensagem, *software* ou documento digital.
Cifragem	O processo de conversão de informações ou dados num código, especialmente para impedir o acesso não autorizado.
Ingestão de ficheiro	O processo de leitura de um ficheiro.
Barreira de segurança (*firewall*)	Dispositivo ou *software* de segurança de rede que monitoriza e controla o tráfego de entrada e saída da rede, com base em regras predefinidas.
Teste de SQE habilitado (*heartbeat*)	Sinal periódico gerado e monitorizado por equipamento informático ou *software* para indicar o funcionamento normal ou para sincronizar outras partes de um sistema informático.
IPSec	Segurança IP. Conjunto de protocolos de rede que autentica e cifra os pacotes de dados para fornecer comunicações cifradas seguras entre dois computadores numa rede IP (Protocolo de Internet).
Testes de penetração	Prática de testar um sistema informático, rede ou aplicação Web para detetar vulnerabilidades de segurança que um atacante poderia explorar.
Processo de conciliação	Processo que visa garantir que dois conjuntos de registos estão de acordo.
RPV	Rede privada virtual.
XML	Linguagem de Marcação Extensível. Permite aos programadores criar as suas próprias etiquetas (*tags*) personalizadas, possibilitando a definição, transmissão, validação e interpretação de dados entre aplicações e organizações.

2. **Introdução**

O Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa, de 23 de novembro de 2017 («Acordo»), prevê o reconhecimento mútuo das licenças de emissão que possam ser utilizadas para efeitos de conformidade ao abrigo do regime de comércio de licenças de emissão da União Europeia («RCLE-UE») [cuja designação foi entretanto alterada para «sistema de comércio de licenças de emissão da União», com o acrónimo «CELE»] ou do sistema de comércio de licenças de emissão da Suíça («RCLE da Suíça»). Com vista a operacionalizar a ligação entre o CELE e o RCLE da Suíça, é estabelecida uma ligação direta entre o Diário de Operações da União Europeia (DOUE) do Registo da União e o Diário de Operações Complementares da Suíça (DOCS) do Registo Suíço, que permitirá a transferência entre registos das licenças de emissão atribuídas ao abrigo de cada um dos sistemas (artigo 3.º, n.º 2, do Acordo). Para que a ligação entre o CELE e o RCLE da Suíça se torne operacional, deve ser adotada uma solução provisória até maio de 2020 ou o mais rapidamente possível após essa data. As Partes devem cooperar para substituir, com a maior brevidade, a solução provisória pela ligação permanente entre registos (anexo II do Acordo).

Nos termos do artigo 3.º, n.º 7, do Acordo, o administrador do Registo Suíço e o administrador central do Registo da União elaboram normas técnicas de ligação (NTL) com base nos princípios enunciados no anexo II do Acordo, descrevendo pormenorizadamente os requisitos relativos ao estabelecimento de uma conexão sólida e segura entre o DOCS e o DOUE. As NTL elaboradas pelos administradores produzem efeitos logo que a decisão do Comité Misto seja adotada.

As NTL, tal como constam do presente documento, deverão ser adotadas pelo Comité Misto através da sua Decisão n.º 2/2020. Em conformidade com esta decisão, o Comité Misto deve solicitar ao administrador do Registo Suíço e ao administrador central do Registo da União que elaborem novas orientações técnicas para operacionalizar a ligação e que assegurem que estas sejam continuamente adaptadas aos progressos técnicos e aos novos requisitos relativos à segurança da ligação e ao seu funcionamento eficaz e eficiente.

2.1. *Âmbito de aplicação*

O presente documento representa o entendimento comum entre as Partes no Acordo sobre o estabelecimento das bases técnicas da ligação entre os registos do CELE e do RCLE da Suíça. Embora defina a linha de base das especificações técnicas em termos de requisitos de arquitetura, serviço e segurança, serão necessárias orientações mais pormenorizadas para tornar a ligação operacional.

Para assegurar o bom funcionamento da ligação, importa definir processos e procedimentos que a tornem ainda mais operacional. Nos termos do artigo 3.º, n.º 6, do Acordo, essas questões são especificadas num documento que define os procedimentos operacionais comuns (POC), a adotar separadamente por decisão do Comité Misto.

2.2. *Destinatários*

Os destinatários do presente documento são o administrador do Registo Suíço e o administrador central do Registo da União.

3. **Disposições gerais**

3.1. *Arquitetura da ligação de comunicação*

O objetivo da presente secção é fornecer uma descrição da arquitetura geral da operacionalização da ligação entre o CELE e o RCLE da Suíça, bem como das diferentes componentes envolvidas na mesma.

Uma vez que a segurança é parte essencial da definição da arquitetura da ligação entre registos, foram adotadas todas as medidas para dispor de uma arquitetura sólida. Embora a ligação permanente entre registos prevista se baseie em serviços Web, a solução provisória utilizará um mecanismo de troca de ficheiros.

A solução técnica utiliza:

— um protocolo seguro de transferência de mensagens,

— mensagens XML,

— assinatura digital e cifragem baseadas em XML,

— dispositivo RPV ou rede segura de transporte de dados equivalente.

3.1.1. Troca de mensagens

A comunicação entre o Registo da União e o Registo Suíço basear-se-á num mecanismo de troca de mensagens através de canais protegidos. Cada extremidade contará com o seu próprio repositório de mensagens recebidas.

Ambas as Partes manterão um diário das mensagens recebidas, juntamente com os dados de tratamento.

Os erros ou estados inesperados devem ser comunicados, sob a forma de alertas, e as equipas de apoio devem estar em contacto.

Os erros e eventos inesperados serão tratados de acordo com os procedimentos operacionais estabelecidos no processo de gestão de incidentes dos POC.

3.1.2. Mensagem XML — Descrição de alto nível

Uma Mensagem XML contém um dos seguintes elementos:

— um ou vários pedidos de operações e/ou uma ou várias respostas a operações,

— uma operação/resposta relacionada com a conciliação,

— uma mensagem de teste.

Todas as mensagens contêm um cabeçalho com os seguintes elementos:

— sistema RCLE de origem,

— número sequencial.

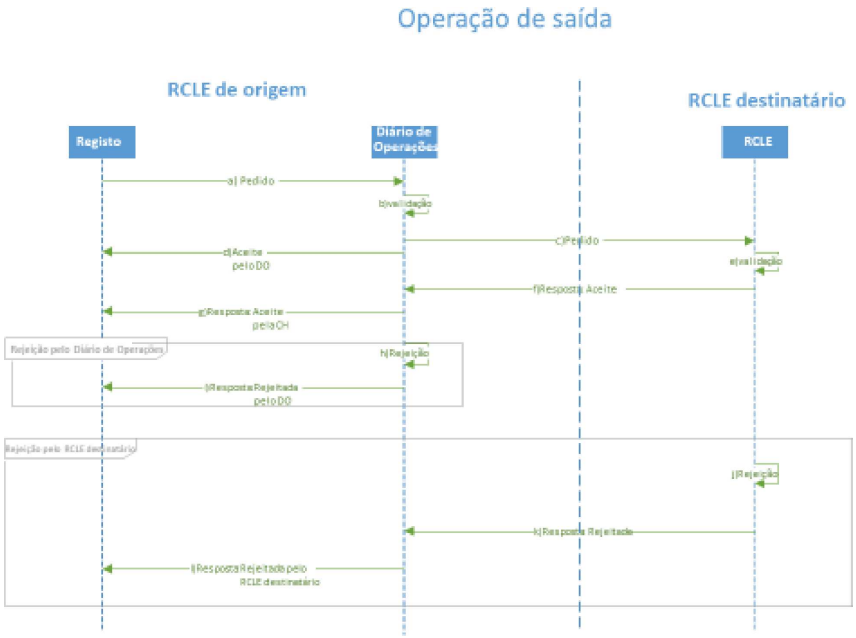
3.1.3. Períodos de ingestão

A solução provisória baseia-se em períodos de ingestão predefinidos, seguidos de um conjunto de eventos designados. Os pedidos de operações recebidos através da ligação apenas serão ingeridos em intervalos predefinidos. Os períodos de ingestão incluem uma validação técnica das operações à saída e à entrada. Além disso, as conciliações podem ser executadas diariamente e acionadas manualmente.

As alterações da frequência e/ou do momento de realização de quaisquer destes eventos serão tratadas de acordo com os procedimentos operacionais estabelecidos no processo de cumprimento de pedidos dos POC.

3.1.4. Fluxos de mensagens de operações

Operações de saída



Esta secção reflete o ponto de vista do RCLE de origem da transferência. O diagrama sequencial acima ilustra todos os fluxos específicos de operações de saída.

Fluxo principal «Operação Normal» (com as etapas indicadas na imagem acima):

a) No RCLE de origem da transferência, o pedido de operação é enviado do registo para o diário de operações, após o término de todos os prazos previstos para a atividade comercial (período de 24 horas, quando aplicável);

b) O diário de operações valida o pedido de operação;

c) O pedido de operação é enviado para o RCLE destinatário;

d) A resposta de aceitação é enviada ao registo do RCLE de origem;

e) O RCLE destinatário valida o pedido de operação;

f) O RCLE destinatário envia a resposta de aceitação ao diário de operações do RCLE de origem;

g) O diário de operações envia a resposta de aceitação ao registo.

Fluxo alternativo «Rejeição do Diário de Operações» [com as etapas indicadas na imagem acima, começando igualmente em a)]:

a) No RCLE de origem, o pedido de operação é enviado do registo para o diário de operações, após o término de todos os prazos previstos para a atividade comercial (período de 24 horas, quando aplicável);

Seguindo-se as etapas:

b) O diário de operações não valida o pedido;

c) A mensagem de rejeição é enviada ao registo de origem.

Fluxo alternativo «Rejeição do RCLE» [com as etapas indicadas na imagem acima, começando em a)]:

a) No RCLE de origem, o pedido de operação é enviado do registo para o diário de operações, após o término de todos os prazos previstos para a atividade comercial (período de 24 horas, quando aplicável);

b) O diário de operações valida a operação;

c) O pedido de operação é enviado para o RCLE destinatário;

d) A mensagem de aceitação é enviada ao registo do RCLE de origem.

Seguindo-se as etapas:

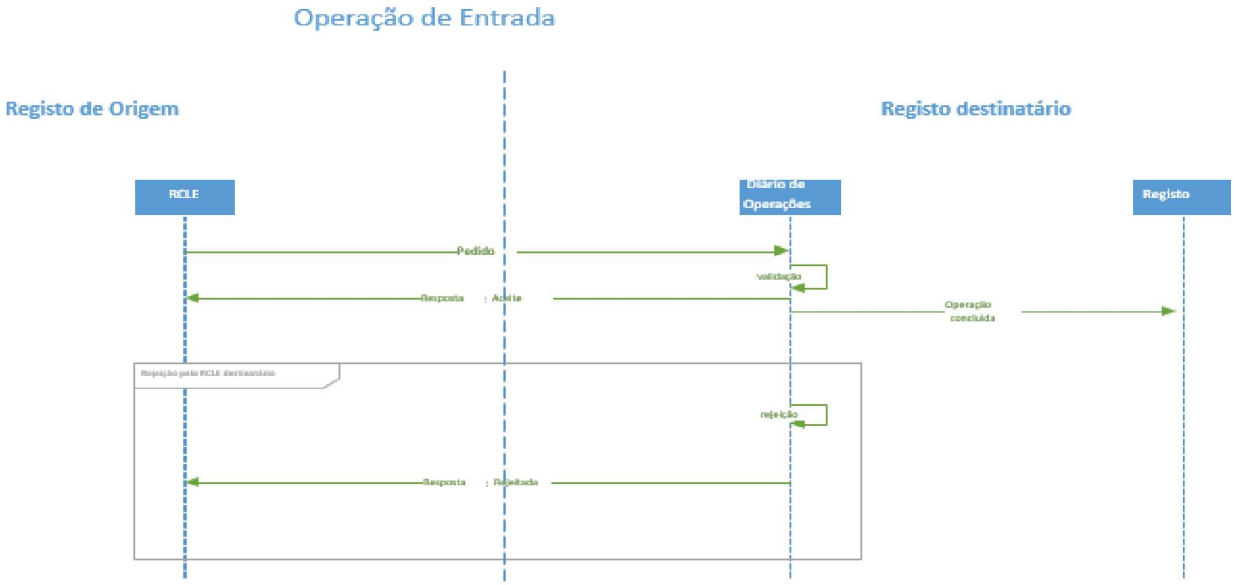
e) O diário de operações do RCLE destinatário da transferência não valida a operação;

f) O RCLE destinatário da transferência envia a resposta de recusa ao diário de operações do RCLE de origem da transferência;

g) O diário de operações envia a recusa ao registo.

Operações de entrada

Esta secção reflete o ponto de vista do RCLE destinatário da transferência. O fluxo específico é ilustrado no seguinte diagrama sequencial:



O diagrama mostra:

1. Quando o diário de operações do RCLE destinatário da transferência valida o pedido, envia a mensagem de aceitação ao RCLE de origem da transferência e uma mensagem de «operação concluída» ao registo do RCLE destinatário;
2. Quando um pedido recebido é recusado no diário de operações do RCLE destinatário da transferência, o pedido de operação não é enviado para o registo correspondente.

Protocolo

O ciclo de mensagens da operação engloba apenas duas mensagens:

— RCLE de origem da transferência Proposta de operação ao RCLE destinatário da transferência.

— RCLE destinatário da transferência Resposta à operação do RCLE de origem da transferência: aceite ou rejeitada (incluindo o motivo da rejeição):

  — aceite: a operação é concluída,

  — rejeitada: a operação é cessada.

Estado da operação

— O estado da operação do RCLE de origem da transferência será definido como «proposta» quando o pedido é enviado.

— O estado da operação do RCLE destinatário da transferência será definido como «proposta» quando o pedido é recebido e durante o seu tratamento.

— O estado da operação do RCLE destinatário da transferência será definido como «concluída»/«cessada» quando a proposta tiver sido tratada. O RCLE destinatário da transferência enviará então a mensagem de aceitação/rejeição correspondente.

— O estado da operação do RCLE de origem da transferência será definido como «concluída»/«cessada» quando a aceitação/rejeição tiver sido recebida e tratada.

— No RCLE de origem da transferência, o estado da operação permanecerá como «proposta» se não for recebida uma resposta.

— O estado da operação do RCLE destinatário da transferência será definido como «cessada» se uma operação estiver no estado «proposta» durante mais de 30 minutos.

Os incidentes relacionados com operações serão tratados de acordo com os procedimentos operacionais estabelecidos no processo de gestão de incidentes dos POC.

3.2. *Segurança da transferência de dados*

Os dados em trânsito serão objeto de quatro níveis de segurança:

1) Controlo do acesso à rede: barreira de segurança e camada de interconexão de redes;

2) Cifragem ao nível do transporte: RPV ou rede segura de transporte de dados equivalente;

3) Cifragem ao nível da sessão: protocolo seguro de transferência de mensagens;

4) Cifragem ao nível da aplicação: cifragem e assinatura de conteúdos XML.

3.2.1. Barreira de segurança e interconexão de redes

A ligação é estabelecida numa rede protegida por uma barreira de segurança (*firewall*) baseada em equipamento informático. A barreira de segurança é configurada com regras, de molde a permitir que apenas os clientes «registados» consigam estabelecer ligações ao servidor da RPV.

3.2.2. Rede privada virtual (RPV)

Todas as comunicações entre as Partes são protegidas com recurso a uma tecnologia segura de transporte de dados. No caso de uma Rede Privada Virtual (RPV), a infraestrutura deve estar baseada em equipamento informático ou em dispositivos virtuais. As tecnologias de RPV permitem criar um «túnel» entre dois pontos, através de uma rede como a Internet, protegendo todas as comunicações. Antes da criação do túnel da RPV, é emitido um certificado digital à extremidade de um potencial cliente, para que forneça uma prova de identidade durante a negociação da ligação. Cada Parte é responsável por instalar o certificado na respetiva extremidade da RPV. Utilizando certificados digitais, cada servidor da RPV de destino irá aceder a uma autoridade central para negociar as credenciais de autenticação. Durante o processo de criação do túnel, a cifragem é negociada, garantindo que todas as comunicações efetuadas através do mesmo são protegidas.

As extremidades da RPV do cliente serão configuradas para manter permanentemente o túnel da RPV, com vista a permitir uma comunicação fiável, bidirecional e em tempo real entre as Partes, em todos os momentos.

Qualquer outra solução equivalente deverá cumprir os princípios mencionados anteriormente.

3.2.3. Execução de IPSec

Caso seja utilizada uma solução de RPV, a aplicação do protocolo IPSec para formar a infraestrutura de RPV «site a site» (*site-to-site*) garantirá a autenticação «site a site», a integridade e a cifragem dos dados. As configurações de IPSec da RPV garantem a devida autenticação entre duas extremidades numa ligação RPV. As Partes irão identificar e autenticar o cliente remoto através da ligação IPSec, utilizando certificados digitais fornecidos por uma autoridade de certificação reconhecida mutuamente.

A IPSec também garante a integridade dos dados de todas as comunicações transmitidas pelo túnel da RPV. Os pacotes de dados são sujeitos a dispersão (*hashed*) e assinados com recurso às informações de autenticação estabelecidas pela RPV. A confidencialidade dos dados é também assegurada através da cifragem IPSec.

3.2.4. Protocolo seguro de transferência para troca de mensagens

A solução provisória recorre a várias camadas de cifragem para permitir a troca segura de dados entre as Partes. Ambos os sistemas e os seus diferentes ambientes são interligados ao nível da rede através de túneis da RPV ou de redes seguras de transporte de dados equivalentes. A nível da aplicação, os ficheiros são transferidos utilizando um protocolo seguro de transferência de mensagens a nível da sessão.

3.2.5. Cifragem e assinatura XML

Nos ficheiros XML, a assinatura e a cifragem ocorrem em dois níveis. Todos os pedidos de operações, respostas a operações e mensagens de conciliação são assinados digitalmente, de forma individual.

Numa segunda etapa, cada subelemento do elemento «mensagem» é cifrado individualmente.

Além disso, numa terceira etapa e para assegurar a integridade e a não rejeição de toda a mensagem, a mensagem do elemento raiz é assinada digitalmente, o que resulta num elevado nível de proteção dos dados incorporados no ficheiro XML. A execução técnica obedece às normas do Consórcio World Wide Web.

Para decifrar e verificar a mensagem, o processo segue a ordem inversa.

3.2.6. Chaves criptográficas

Será utilizada criptografia de chave pública para efeitos de cifragem e assinatura.

No caso específico da IPSec, é utilizado um certificado digital emitido por uma autoridade de certificação (AC) na qual ambas as Partes depositam confiança. Esta AC verifica a identidade do titular do certificado e emite certificados que são utilizados para identificar uma organização com precisão e configurar canais de comunicação de dados seguros entre as Partes.

As chaves criptográficas são utilizadas para assinar e cifrar canais de comunicação e ficheiros de dados. As Partes trocam digitalmente certificados públicos, utilizando canais seguros, que são verificados fora de banda. Este procedimento é parte integrante do processo de gestão da segurança da informação dos POC.

3.3. *Lista de funções ao abrigo da ligação*

A ligação especifica o sistema de transmissão de várias funções que executam os processos comerciais decorrentes do Acordo. Do mesmo modo, inclui especificações relativas ao processo de conciliação e às mensagens de teste que permitirão a execução de um teste de SQE habilitado.

3.3.1. Operações comerciais

Em termos comerciais, a ligação contempla quatro (4) tipos de pedidos de operações:

— Transferência externa:

  — após a entrada em vigor da ligação entre os RCLE, as licenças da UE e da Suíça são fungíveis e, por conseguinte, totalmente transferíveis entre as Partes,

— uma transferência enviada através da ligação irá envolver uma conta de origem num RCLE e uma conta destinatária da transferência no outro RCLE,

— a transferência pode incluir qualquer quantidade dos quatro (4) tipos de licenças:

— licenças de emissão gerais da Suíça (CHU),

— licenças de emissão da aviação da Suíça (CHUA),

— licenças de emissão gerais da UE (LUE),

— licenças emissão da aviação da UE (LUEa).

— Atribuição internacional:

Os operadores de aeronaves geridos por um RCLE com obrigações no outro RCLE e que tenham direito a receber, do segundo, licenças de emissão a título gratuito irão receber licenças de emissão da aviação gratuitas do segundo RCLE através da operação de atribuição internacional.

— Estorno da atribuição internacional:

Esta operação ocorrerá apenas se for necessário estornar na totalidade as licenças de emissão atribuídas a título gratuito à conta de depósito de um operador de aeronaves pelo outro RCLE.

— Restituição dos excedentes atribuídos:

Semelhante ao estorno, mas neste caso não é necessário estornar na íntegra a atribuição, sendo apenas obrigatório restituir as licenças de emissão atribuídas em excesso ao RCLE de origem.

3.3.2. Protocolo de conciliação

As conciliações apenas irão ocorrer após o encerramento dos períodos de ingestão, validação e tratamento de mensagens.

As conciliações são parte integrante das medidas necessárias para assegurar a segurança e a coerência da ligação. As duas Partes acordarão o momento exato da conciliação antes de definir qualquer programação. Se ambas as Partes manifestarem o seu acordo, pode ser programada uma conciliação diária. Será executada, no mínimo, uma conciliação programada após cada ingestão.

Em todo o caso, cada Parte pode iniciar conciliações manuais a qualquer momento.

As alterações do momento e da frequência da conciliação programada serão tratadas de acordo com os procedimentos operacionais estabelecidos no processo de cumprimento de pedidos dos POC.

3.3.3. Mensagem de teste

Está previsto o envio de uma mensagem para testar a comunicação de extremo a extremo. A mensagem irá conter dados que a identificarão como um teste e, uma vez recebida na outra extremidade, receberá uma resposta.

3.4. *Normas para os serviços Web*

Os serviços Web não serão utilizados no âmbito da solução provisória. No entanto, convém salientar que a forma e o formato das mensagens XML permanecerão, em grande medida, inalterados. Com a introdução da ligação permanente entre registos no futuro, os serviços Web devem permitir a troca de mensagens XML em tempo real.

3.5. *Definição específica de serviços Web*

A presente secção não é aplicável à solução provisória. Conforme mencionado na secção anterior, os serviços Web apenas serão utilizados na futura ligação permanente entre registos.

3.6. *Requisitos de registo de dados*

A fim de responder à necessidade, de ambas as Partes, de manter informações exatas e coerentes, bem como de disponibilizar ferramentas para resolver incoerências no âmbito do processo de conciliação, as Partes mantêm quatro (4) tipos de registos de dados:

— diários de operações,

— registos de conciliação,

— arquivo de mensagens,

— registos de auditorias internas.

Todos os dados constantes destes registos são mantidos, no mínimo, durante três (3) meses para fins de resolução de problemas, sendo que a sua conservação posterior irá depender da legislação aplicável em cada extremidade para efeitos de auditoria. Os ficheiros de registo com mais de três (3) meses podem ser arquivados num local seguro, num sistema de TI independente, desde que seja possível recuperá-los ou aceder aos mesmos num prazo razoável.

Diários de operações

Os subsistemas DOUE e DOCS contêm execuções do diário de operações.

Mais especificamente, os diários de operações irão manter um registo de cada operação proposta enviada ao outro RCLE. Cada registo contém todos os campos do conteúdo da operação e o resultado posterior da mesma (a resposta do RCLE que recebe o pedido). Os diários de operações manterão também um registo das entradas de operações, bem como da resposta enviada ao RCLE de origem.

Registos de conciliação

O registo de conciliação contém um registo de cada mensagem de conciliação trocada entre as duas Partes, incluindo a identificação da conciliação, o carimbo temporal e o resultado da conciliação: estado de conciliação «aprovada» ou «discrepâncias». Na solução provisória, as mensagens de conciliação são parte integrante das mensagens trocadas.

As duas Partes devem registar cada pedido e a respetiva resposta no registo de conciliação. Embora as informações deste registo não sejam partilhadas diretamente no âmbito do processo de conciliação propriamente dito, pode ser necessário aceder-lhes para resolver incoerências.

Arquivo de mensagem

Ambas as Partes têm de arquivar uma cópia dos dados trocados (os ficheiros XML), enviados e recebidos, indicando se essas mensagens XML estavam ou não no formato correto.

O arquivo destina-se sobretudo a fins de auditoria, permitindo dispor de um comprovativo do que foi enviado e recebido à/da outra Parte. Nesse sentido, juntamente com os ficheiros, também é necessário arquivar os certificados conexos.

Estes ficheiros fornecerão igualmente informações adicionais para efeitos de resolução de problemas.

Registo de auditoria interna

Estes registos são definidos e utilizados por cada Parte isoladamente.

3.7. *Requisitos operacionais*

Na solução provisória, a troca de dados entre os dois sistemas não é totalmente autónoma, ou seja, são necessários operadores e procedimentos para operacionalizar a ligação.

4. **Disposições em matéria de disponibilidade**

4.1. *Conceção que garante a disponibilidade das comunicações*

A arquitetura da solução provisória consiste, fundamentalmente, numa infraestrutura de TIC e *software* que permitem a comunicação entre o RCLE da Suíça e o CELE. Garantir elevados níveis de disponibilidade, integridade e confidencialidade deste fluxo de dados torna-se, por conseguinte, um aspeto essencial a considerar na conceção da solução provisória e da ligação permanente entre registos. Uma vez que se trata de um projeto em que a infraestrutura de TIC, o *software* personalizado e os processos desempenham um papel fundamental, é necessário ter em conta os três elementos para criar um sistema resiliente.

Resiliência da infraestrutura de TIC

O capítulo do presente documento intitulado «Disposições gerais» descreve em pormenor os elementos de base da arquitetura. Ao nível da infraestrutura de TIC, a ligação provisória estabelece uma rede RPV (ou equivalente) resiliente, que cria túneis de comunicação seguros, nos quais podem ocorrer trocas de mensagens em segurança. Outros elementos da infraestrutura são configurados em alta disponibilidade e/ou contam com mecanismos de reparação de falhas.

Resiliência do *software* personalizado

Os módulos de *software* personalizados reforçam a resiliência, uma vez que tentam restabelecer a comunicação com a outra extremidade durante um determinado período se, por qualquer motivo, esta não estiver disponível.

Resiliência do serviço

Na solução provisória, as trocas de dados entre as Partes ocorrem em intervalos de tempo predefinidos ao longo do ano. Algumas das etapas necessárias nas trocas de dados programadas exigem a intervenção manual dos operadores do sistema e/ou dos administradores dos registos. Tendo em conta este aspeto e para aumentar e disponibilidade e o êxito das trocas:

— os procedimentos operacionais preveem períodos de tempo significativos para realizar cada etapa,

— os módulos de *software* da solução provisória executam uma comunicação assíncrona,

— o processo de conciliação automático irá detetar se ocorreram problemas na ingestão dos ficheiros de dados em ambas as extremidades,

— os processos de monitorização (infraestrutura de TIC e módulos de *software* personalizados) são considerados e ativam os procedimentos de gestão de incidentes (conforme definidos no documento relativo aos procedimentos operacionais comuns). Esses procedimentos, que visam reduzir o tempo necessário para restabelecer o funcionamento normal após a ocorrência de incidentes, são essenciais para assegurar índices de disponibilidade elevados.

4.2. *Inicialização, comunicação, reativação e plano de teste*

Os diferentes elementos envolvidos na arquitetura da solução provisória são, todos eles, submetidos a vários testes individuais e coletivos, para confirmar que a plataforma está pronta ao nível da infraestrutura de TIC e do sistema de informação. Estes testes de operacionalidade são um pré-requisito obrigatório sempre que a plataforma altera o estado da solução provisória de suspenso para operacional.

A ativação do estado operacional da ligação exige então uma execução bem-sucedida de um plano de teste predefinido, que confirmará que cada registo realizou primeiramente um conjunto de testes internos, seguido de uma validação da conectividade de extremo a extremo, antes de iniciar a apresentação de operações reais entre ambas as Partes.

O plano de teste deve mencionar a estratégia geral de teste e informações pormenorizadas sobre a infraestrutura de teste, nomeadamente, deve incluir, para cada elemento em todos os blocos de teste:

— os critérios de teste e as respetivas ferramentas,

— as funções atribuídas para a realização do teste,

— os resultados previstos (positivos e negativos),

— a programação do teste,

— os requisitos de registo dos resultados do teste,

— documentação de resolução de problemas,

— disposições em matéria de escalonamento.

Enquanto processo, os testes de ativação do estado operacional podem ser divididos em quatro (4) blocos conceptuais ou fases:

4.2.1. Testes da infraestrutura de TIC interna

Estes testes destinam-se a ser realizados e/ou verificados individualmente por ambas as Partes, em cada extremidade.

Todos os elementos da infraestrutura de TIC, em cada extremidade, são testados individualmente, incluindo cada componente da infraestrutura. Estes testes podem ser executados de forma automática ou manual, devendo verificar que todos os elementos da infraestrutura estão operacionais.

4.2.2. Testes das comunicações

Estes testes são acionados individualmente por qualquer uma das Partes e a sua conclusão exige a cooperação da outra extremidade.

Quando os elementos individuais estiverem operacionais, será necessário testar os canais de comunicação entre os dois registos. Para este fim, cada Parte deverá verificar que o acesso à Internet funciona, que os túneis da RPV (ou rede segura de transporte equivalente) estão estabelecidos e que há conectividade IP «site a site». A acessibilidade dos elementos da infraestrutura locais e remotos e a conectividade IP devem então ser confirmadas na outra extremidade.

4.2.3. Testes do sistema completo (de extremo a extremo)

Estes testes destinam-se a ser executados em cada extremidade e os resultados são partilhados com a contraparte.

Quando os canais de comunicação e todos os componentes individuais de ambos os registos tiverem sido testados, cada extremidade irá preparar uma série de operações e conciliações simuladas, representativas de todas as funções a executar no âmbito da ligação.

4.2.4. Testes da segurança

Estes testes destinam-se a ser realizados ou acionados por ambas as Partes em cada extremidade, conforme indicado em pormenor nas secções 5.4 («Orientações relativas a testes da segurança») e 5.5 («Disposições em matéria de avaliação de riscos»).

Só se poderá considerar que a ligação provisória está operacional quando as quatro fases/blocos terminarem com resultados previsíveis.

Recursos de teste

Cada Parte deve contar com recursos de teste específicos (*software* e equipamento informático específicos da infraestrutura de TIC) e desenvolver funções de teste no respetivo sistema, para apoiar a validação manual e contínua da plataforma. Os procedimentos de teste manuais, realizados individualmente ou em cooperação, podem ser executados em qualquer altura pelos administradores dos registos. A ativação do estado operacional é, em si, um processo manual.

Também está previsto que a plataforma realize verificações automáticas regularmente. Essas verificações destinam-se a aumentar a disponibilidade da plataforma, ao detetar precocemente potenciais problemas ao nível da infraestrutura ou do *software*. Este plano de monitorização da plataforma é composto por dois elementos:

— monitorização das infraestruturas de TIC: em ambas as extremidades, os prestadores de serviços da infraestrutura de TIC procederão à sua monitorização. Os testes automáticos irão abranger os diferentes elementos da infraestrutura e a disponibilidade dos canais de comunicação,

— monitorização da aplicação: os módulos do *software* da ligação provisória irão executar uma monitorização das comunicações do sistema ao nível da aplicação (manualmente e/ou em intervalos regulares), que permitirá testar a disponibilidade da ligação de extremo a extremo simulando algumas das operações.

4.3. *Ambientes de aceitação/teste*

A arquitetura do Registo da União e do Registo Suíço é constituída pelos seguintes três ambientes:

— produção (PROD): este ambiente contém os dados reais e processa operações reais,

— aceitação (ACEIT): este ambiente contém dados representativos não reais ou anonimizados. É o ambiente onde os operadores do sistema de ambas as Partes validam as novas versões,

— teste (TEST): este ambiente contém dados representativos não reais ou anonimizados. O seu acesso está limitado aos administradores dos registos e destina-se à realização de testes de integração por ambas as Partes.

Exceto no que respeita à RPV (ou rede equivalente), os três ambientes são totalmente independentes uns dos outros, o que significa que o equipamento informático, o *software*, as bases de dados, os ambientes virtuais, os endereços IP e as portas são configurados e funcionam independentemente.

No que se refere ao esquema, a RPV está configurada em dois ambientes diferentes: um de PROD e outro independente para ACEIT e TEST.

5. **Disposições em matéria de confidencialidade e integridade**

Os mecanismos e procedimentos de segurança preveem um método que envolve duas pessoas (princípio dos «quatro olhos») para operações que ocorram na ligação entre o Registo da União e o Registo Suíço. Este método aplica-se sempre que necessário. No entanto, pode não ser aplicável a todas as etapas realizadas pelos administradores dos registos.

Os requisitos de segurança são considerados e tratados no plano de gestão da segurança, que inclui igualmente processos relacionados com o tratamento dos incidentes de segurança na sequência de uma eventual violação da segurança. A parte operacional destes processos é descrita nos POC.

5.1. *Infraestrutura de teste da segurança*

Cada Parte compromete-se a estabelecer uma infraestrutura de teste da segurança (recorrendo ao *software* e ao equipamento informático comuns utilizados na deteção de vulnerabilidades nas etapas de desenvolvimento e funcionamento):

— separada do ambiente de produção,

— em que a segurança é analisada por uma equipa independente do desenvolvimento e funcionamento do sistema.

Cada Parte compromete-se a realizar análises estáticas e dinâmicas.

No caso das análises dinâmicas (como os testes de penetração), as duas Partes comprometem-se a limitar as avaliações normalmente realizadas aos ambientes de teste e de aceitação (conforme definidos na secção 4.3, «Ambientes de aceitação/teste»). As exceções à presente política estão sujeitas à aprovação das duas Partes.

Antes de serem implantados no ambiente de produção, todos os módulos de *software* da ligação (conforme definidos na secção 3.1, «Arquitetura da ligação de comunicação») são submetidos a testes de segurança.

A infraestrutura de teste tem de ser separada, a nível da rede e da infraestrutura, da infraestrutura de produção. Os testes de segurança necessários para verificar o cumprimento dos requisitos de segurança são realizados na infraestrutura de teste.

5.2. *Disposições em matéria de suspensão e reativação da ligação*

Caso exista uma suspeita de que a segurança do Registo Suíço, do DOCS, do Registo da União ou do DOUE esteja comprometida, ambas as Partes informarão imediatamente a outra Parte e suspenderão a ligação entre o DOCS e o DOUE.

Os procedimentos para a partilha de informações, a decisão de suspender e a decisão de reativar fazem parte do processo de cumprimento de pedidos dos POC.

Suspensões

A suspensão da ligação entre registos, em conformidade com o anexo II do Acordo, pode ocorrer devido a:

— motivos administrativos (por exemplo, manutenção) planeados,

— motivos de segurança (ou falhas na infraestrutura de TI) não planeados.

Em caso de emergência, cada Parte informará a outra e suspenderá unilateralmente a ligação entre registos.

Se for tomada a decisão de suspender a ligação entre registos, cada Parte irá assegurar que a ligação é interrompida a nível da rede (bloqueando parcialmente ou na totalidade as ligações de entrada e de saída).

A decisão de suspender a ligação entre registos, independentemente de ser ou não planeada, será tomada de acordo com os procedimentos de gestão de alterações ou de gestão de incidentes de segurança dos POC.

Reativação da comunicação

A decisão de reativação da ligação entre registos será tomada conforme descrito em pormenor nos POC e nunca antes de os procedimentos de teste da segurança (conforme indicados nas secções «Orientações relativas aos testes da segurança» e «Inicialização, comunicação, reativação e plano de teste») terem sido concluídos com êxito.

5.3. *Disposições em matéria de violação da segurança*

Uma violação da segurança é um incidente de segurança que afeta a confidencialidade e a integridade de informações sensíveis e/ou a disponibilidade do sistema que as trata.

As informações sensíveis são identificadas na lista de informações sensíveis e podem ser tratadas no sistema ou em qualquer parte conexa do mesmo.

As informações diretamente relacionadas com a violação da segurança serão consideradas sensíveis, assinaladas com «RCLE CRÍTICO» e tratadas de acordo com as instruções de tratamento, salvo indicação em contrário.

Todas as violações da segurança serão tratadas em conformidade com o capítulo dos POC dedicado à gestão de incidentes de segurança.

5.4. *Orientações relativas aos testes da segurança*

5.4.1. Programas informáticos (*software*)

Todas as novas versões importantes do *software* são sujeitas a testes de segurança, incluindo testes de penetração, se aplicáveis, em conformidade com os requisitos de segurança estabelecidos nas NTL, a fim de avaliar a segurança da ligação e os riscos associados.

Se não tiver sido produzida nenhuma versão importante nos últimos 12 meses, é realizado um teste da segurança do sistema atual que tenha em conta a evolução das ciberameaças ao longo desse período.

Os testes da segurança da ligação entre registos são realizados no ambiente de aceitação e, se necessário, no ambiente de produção, com a coordenação e o acordo mútuo de ambas as Partes.

Os testes da aplicação Web respeitarão as normas abertas internacionais, tais como as desenvolvidas pelo Projeto de Segurança de Aplicações Web Abertas (*Open Web Application Security Project*, OWASP).

5.4.2. Infraestrutura

A infraestrutura de apoio ao sistema de produção será analisada regularmente para identificar vulnerabilidades (no mínimo, uma vez por mês) e as vulnerabilidades detetadas serão corrigidas. Os testes são realizados de acordo com o método descrito na secção 5.4.1, utilizando uma base de dados de vulnerabilidades atualizada.

5.5. *Disposições em matéria de avaliação de riscos*

Se estiverem disponíveis testes de penetração, estes devem ser incluídos nos testes da segurança.

Cada Parte pode contratar uma empresa especializada com vista à realização dos testes da segurança, desde que a mesma:

— disponha das competências e da experiência necessárias para a realização desses testes da segurança,

— não esteja subordinada diretamente ao programador e/ou ao seu contratante, não esteja envolvida no desenvolvimento do *software* da ligação, nem seja uma subcontratante do programador,

— tenha assinado um acordo de confidencialidade para manter os resultados confidenciais e os tratar de acordo com o nível «RCLE CRÍTICO» e as instruções de tratamento.