GRC·RCMP
GENDARMERIE ROYALE DU CANADA • ROYAL CANADIAN MOUNTED POLICE

Projet de biométrie pour les résidents temporaires et d'identification en temps réel

SPÉCIFICATIONS DE L'INTERFACE DU SOUS-SYSTÈME DE VÉRIFICATION DE LA BIOMÉTRIE POUR LES RÉSIDENTS TEMPORAIRES

CONCEPTION TECHNIQUE

Dernière mise à jour : 2013-03-22
État : Version finale
SRT : REB-11
Version : 1.2
Nº SGDDI : 38553-v7
Classification : Protégé A

REGISTRE DES MODIFICATIONS

TABLE DES MATIÈRES

FIGURES

1. INTRODUCTION

1.1 OBJET

Le présent document présente les spécifications de l'interface du sous-système de vérification (SSV) de la biométrie pour les résidents temporaires (BRT). Ce sous-système doit être compatible avec l'interface entre l'Agence des services frontaliers du Canada (ASFC) et la Gendarmerie royale du Canada (GRC). De plus, son interface doit permettre la communication avec la GRC.

1.2 PORTÉE

Le présent document présente les spécifications d'interface que devront respecter l'ASFC et la GRC et auxquelles il faudra répondre dans le SSV pour permettre la communication par l'intermédiaire de ce sous-système.

1.3 PUBLIC CIBLE

Le présent document est destiné : à l'ASFC; aux parties intéressées à répondre à la demande de propositions (DP) relative au renouvellement du Système automatisé d'identification dactyloscopique (SAID); aux membres de l'équipe du Projet de BRT et d'identification en temps réel (ITR) qui sont appelés à passer en revue et à approuver les décisions de conception touchant la BRT.

1.4 DOCUMENTS DE RÉFÉRENCE PERTINENTS

La rédaction du présent document s'est appuyée sur les documents suivants :

- Document de contrôle d'interface NIST des Services nationaux de police (ou DCI de la BRT), versions 2.1.0 et 2.1.1; n^{os} SGDDI 35766 et 40361;
- TRB Functional and Non-Functional Requirements (RTID/TRB Arch Team Design Approval); n^{o} SGDDI 36612;
- TRB Verification WS RCMP Front End Design; n^{o} SGDDI 38422.

2. CONTEXTE

2.1 APERÇU

Il faut un sous-système assurant la vérification un à un, en temps réel, des empreintes digitales des résidents temporaires transmises par un point d'entrée (PDE) de l'ASFC.

Le modèle d'interface recommandé et approuvé par la Sous-direction de la sécurité ministérielle est présenté dans le document « TRB Verification Web Service (WS) RCMP Front End Design ». Le modèle en question, qui doit répondre aux spécifications, est décrit dans le présent document.

2.2 EXIGENCES OPÉRATIONNELLES, EXIGENCES TECHNIQUES ET EXIGENCES RELATIVES À LA SÉCURITÉ

Le modèle d'interface approuvé du sous-système répond à l'intégralité des exigences opérationnelles, exigences techniques et exigences relatives à la sécurité de la vérification de la BRT.

L'interface du SSV :

- gère les envois simultanés de données par des dactyloscopieuses électroniques situées à différents PDE;
- traite de façon entièrement automatisée des transactions de vérification;
- traite une transaction et renvoie une réponse à l'ASFC dans un délai maximal de 30 secondes;
- traite chaque transaction de vérification et la réponse subséquente de façon synchrone, dans une même session sécurisée;
- renvoie un message d'erreur technique au service Web de l'ASFC à la suite de transactions ayant échoué, si le message d'erreur au service Web ne peut être acheminé;
- est facilement extensible, de manière à répondre à l'augmentation du volume découlant de l'éventuelle mise en place du sous-système dans tous les PDE;
- prend en charge les données « Protégé B » traitées par le SSV;
- présente une disponibilité ininterrompue, même en cas de défaillance, grâce à la redondance des composants au site primaire et au site de reprise après sinistre;
- assure la détection des virus dans toutes les données transmises à l'ASFC;
- assure l'équilibrage de la charge de traitement des transactions entre le site primaire et le site de reprise après sinistre;
- vérifie que les transactions de vérification proviennent bel et bien d'une agence autorisée;
- assure l'intégrité des données de vérification communiquée par l'ASFC à la GRC, et vice versa.

3. MODÈLE DU SOUS-SYSTÈME DE VÉRIFICATION

3.1 INTRODUCTION

Le SSV est capable d'assurer une identification en temps réel (ITR). Il n'y avait aucune obligation de recourir à l'interface actuelle des organismes d'ITR. Cette interface avait notamment été conçue pour traiter en deux heures la plupart des transmissions. C'est pourquoi on a jugé qu'elle ne pourrait pas répondre au délai de 30 secondes exigé.

3.2 EXTRÉMITÉ DANS LE MODULE ACE DES COMMUTATEURS DE COUCHE 3 DE CISCO

Le diagramme ci-dessous (Figure 1) illustre le modèle qui permet d'assurer une interface sécurisée (par service Web) entre l'ASFC et le SSV. L'extrémité de la session SSL se trouve dans le module Application Control Engine (ACE) des commutateurs de couche 3 de Cisco.

Nous décrivons dans les lignes qui suivent le modèle ainsi que les raisons pour lesquelles il répond à toutes les exigences. Puisque l'extrémité de la session SSL se trouve dans la zone démilitarisée (DMZ), le modèle est suffisamment flexible pour permettre la détection des virus, l'utilisation du coupe-feu interne et la répartition de la charge (lors du traitement de la requête par l'équilibreur de charge). La Sous-direction de la sécurité ministérielle a approuvé l'utilisation de ce modèle dans le Projet de BRT. En outre, le modèle a été certifié et homologué par la GRC.

- Un lien sécurisé (par service Web) entre l'ASFC et le module ACE de Cisco est établi et maintenu.
- Ce lien prend la forme d'un lien RPV IPSec à partir de l'ASFC, qui permet la non-répudiation. C'est pourquoi il n'est pas nécessaire d'accompagner les données transmises d'une signature numérique.
- Un point d'entrée transmet au service Web de l'ASFC un paquet NIST de vérification pour effectuer une recherche dactyloscopique dans les empreintes enregistrées. Les empreintes ont été prises au moment où la personne a présenté sa demande de résidence temporaire.
- Le service Web de l'ASFC transmet, pour le compte du point d'entrée, une transaction de vérification d'empreintes. Cette transmission comprend le paquet NIST.
- Le module ACE de Cisco reçoit la transaction de recherche et transmet le paquet NIST en clair au détecteur de virus. Le paquet passe ensuite par divers composants de sécurité des commutateurs de couche 3 de Cisco. Les commutateurs de couche 3 transmettent le paquet à l'un des serveurs Web du SSV.
- Le serveur Web envoie une demande à l'un des serveurs fonctionnels du SSV capables de réaliser une vérification un à un.
- Le serveur fonctionnel renvoie au serveur Web les résultats de la recherche.
- La réponse est retransmise par le serveur Web du SSV au module ACE, qui la retransmet au service Web de l'ASFC (par le lien synchrone), qui la retransmet au point d'entrée.

Remarque : L'illustration ne rend pas compte de l'intégralité du modèle du SSV. Ce qui est illustré vise à expliquer chacune des parties de l'interface.

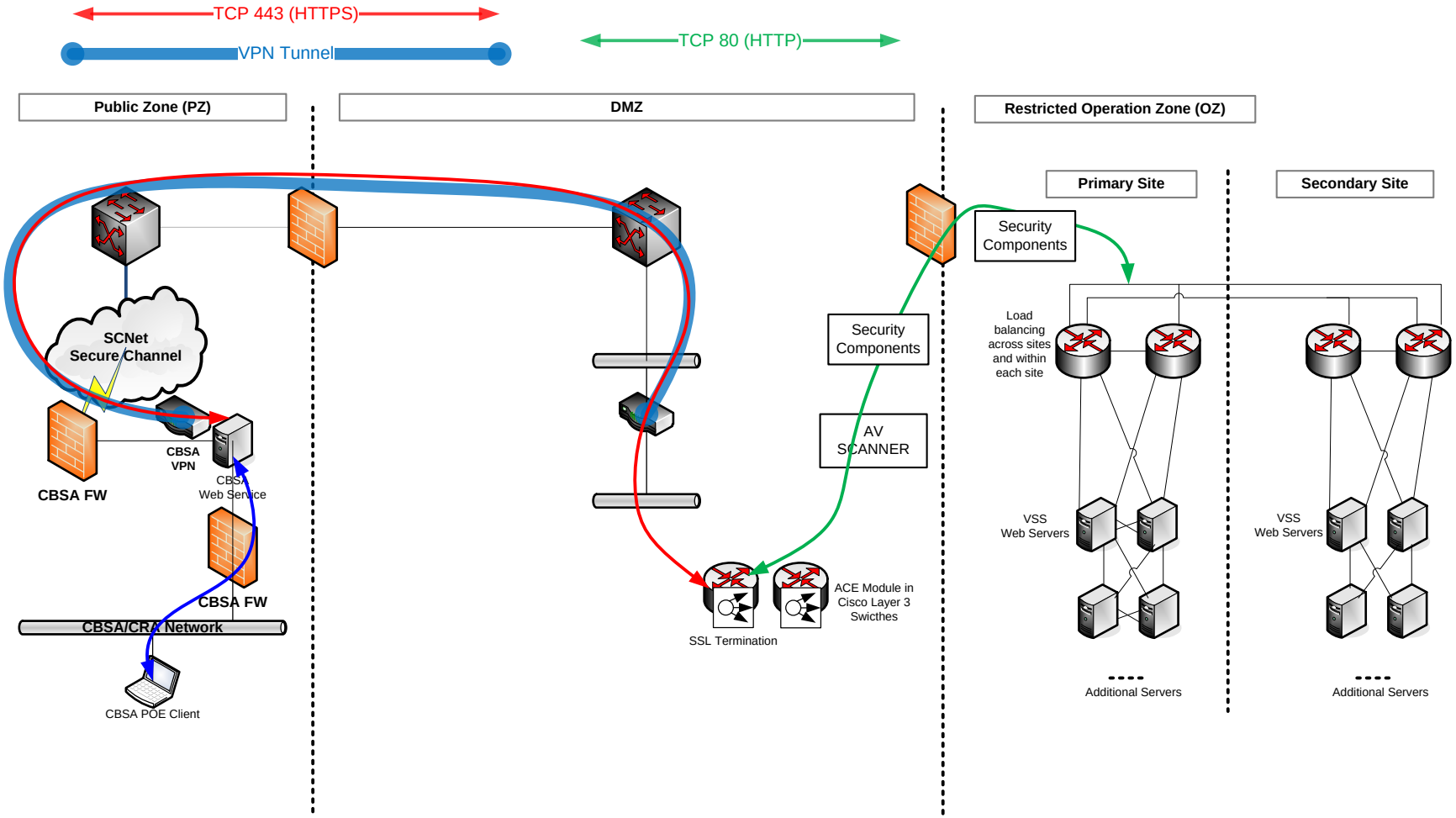

Figure 1 : Modèle du sous-système de vérification

La vitesse est la caractéristique la plus importante du SSV de la BRT. Le niveau de service est fixé à 30 secondes. Ce délai inclut la réception des données, l'envoi de la demande aux serveurs Web du SSV, la réception de la réponse de ces serveurs Web et sa transmission à l'ASFC. Réduire le traitement nécessaire est donc essentiel. Une architecture REST (transfert d'état représentationnel) est simple et permet de réduire à presque rien le temps système. Elle répond à l'intégralité des exigences de la BRT et elle est considérée comme la mieux adaptée à l'interface du SSV de la BRT. Voici les principaux avantages du modèle du SSV :

- Le module ACE des commutateurs de couche 3 de Cisco peut servir d'extrémité à la session SSL. Ses composants matériels et logiciels utilisent des algorithmes d'accélération SSL qui rendent les sessions HTTPS plus rapides que les sessions HTTP en texte clair;
- Dans la configuration de base de la GRC et de SPC, le module ACE traite 1 000 transactions par secondes. Ce chiffre peut passer à 15 000 par une mise à niveau de la licence;
- Étant donné que l'extrémité de la session SSL se trouve dans le module ACE des commutateurs, il est possible d'exécuter une détection de virus et certains autres contrôles de sécurité avant de transmettre les données déchiffrées aux serveurs Web du SSV;
- Le module ACE est doté de caractéristiques comparables à celles de coupe-feu de pointe. Il peut donc inspecter les paquets et assurer une protection contre les attaques par déni de service, entre autres fonctions de sécurité;
- Les commutateurs de couche 3 de Cisco équipés du module ACE étant au cœur de l'infrastructure de la GRC, la solution est pleinement redondante et capable d'assurer le basculement en cas de sinistre.

4. SPÉCIFICATIONS DE L'INTERFACE DE VÉRIFICATION

4.1 APERÇU

La performance est la principale mesure de l'efficacité de l'interface du SSV. C'est pourquoi nous avons établi les spécifications qui suivent dans une volonté d'obtenir l'interface la plus simple et la plus rapide possible tout en respectant les exigences de l'ASFC, de la GRC et du SSV.

Les grandes lignes de ces spécifications sont illustrées dans le diagramme ci-dessous.

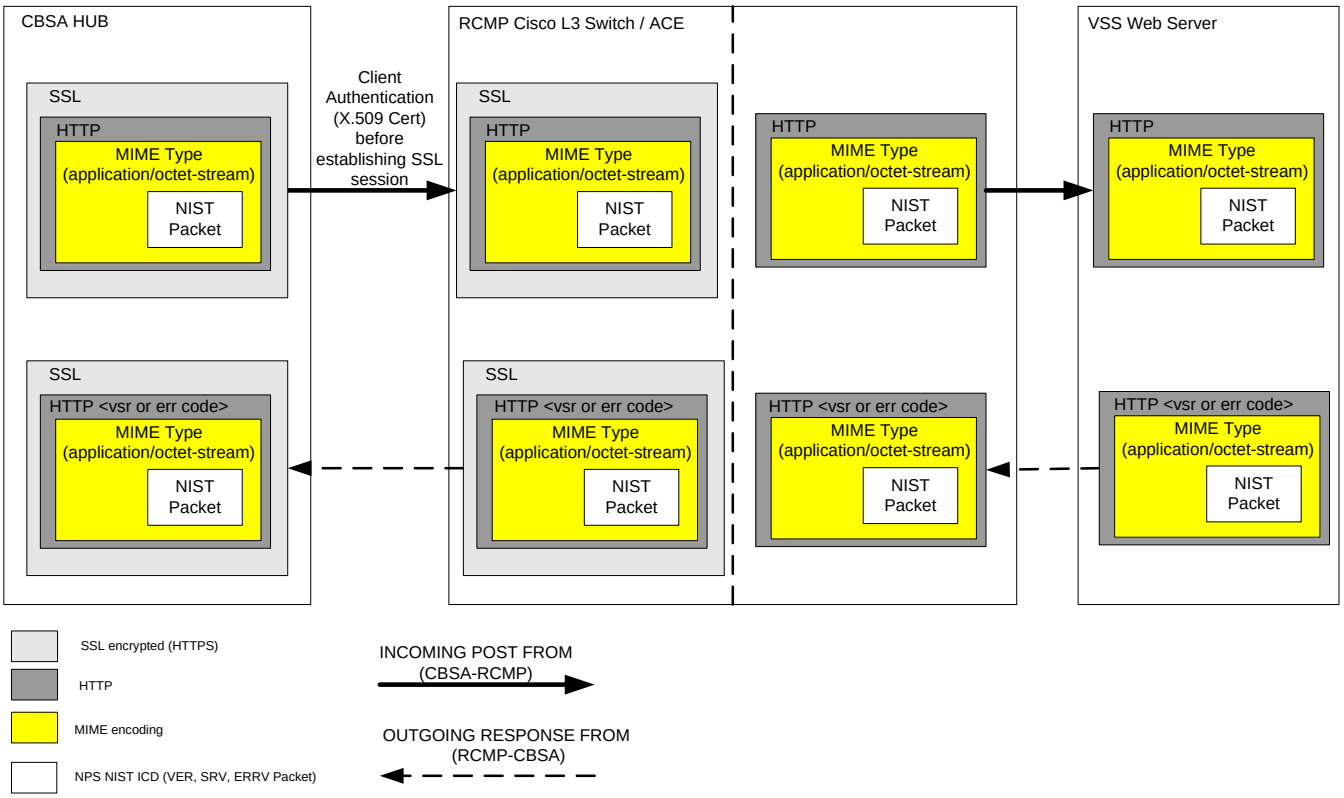

Figure 2 : Spécifications générales de l'interface du SSV

Les spécifications générales de l'interface touchent les éléments suivants :

- l'authentification du client au moyen du certificat X.509 du service Web de l'ASFC;
- l'établissement d'une session SSL entre le service Web de l'ASFC et le commutateur de couche 3 de la GRC (équipé du module ACE), dans la zone démilitarisée de la GRC;
- l'envoi par HTTP, au moyen d'une demande POST, d'un paquet NIST (transaction de vérification [VER]) binaire chiffré selon le protocole MIME;
- le retrait de la couche SSL par le module ACE du commutateur de couche 3, puis la transmission en clair de la demande POST aux serveurs Web du SSV;
- la réception par le serveur Web du SSV du paquet NIST (transaction de vérification [VER]) binaire HTTP chiffré selon le protocole MIME, le déchiffrage du paquet et son envoi aux serveurs fonctionnels du SSV capables de réaliser une vérification un à un;

- la réponse (fondée sur le résultat de la recherche) à la demande POST HTTP par le serveur Web du SSV, sous la forme d'un paquet NIST (transaction SRV ou ERRV) chiffré selon le protocole MIME. L'en-tête HTTP comprend le code VSR ou un code d'erreur;
- l'ajout, par le module ACE du commutateur de couche 3 de Cisco, d'une couche SSL à la réponse du serveur Web du SSV, puis l'envoi de la réponse au service Web de l'ASFC.

4.2 SPÉCIFICATIONS DÉTAILLÉES

Les spécifications détaillées de la transaction VER entrante (sous forme de demande POST HTTP) et de la réponse correspondante sont présentées dans les sous-sections qui suivent. L'objectif consiste à fournir suffisamment de renseignements pour s'assurer que l'ASFC et l'entrepreneur du SSV peuvent terminer leur développement respectif. Il ne s'agit pas de décrire la séquence complète d'interaction des protocoles TCP/IP, HTTP et SSL, mais plutôt de fournir les spécifications clés de l'interface. On s'attend à ce que l'ASFC et l'entrepreneur du SSV connaissent à fond ces protocoles.

4.2.1 CERTIFICATS X.509

Un certificat X.509 créé à l'aide d'une infrastructure à clés publiques (ICP), lequel effectuera l'authentification au moyen de justificatifs d'identité, est nécessaire pour établir une session SSL avec le module ACE du commutateur de couche 3 de Cisco de la GRC. Le certificat du service Web de l'ASFC doit provenir d'une autorité de certification (AC) de confiance de la GRC. Le certificat X.509 doit être délivré par l'AC de l'ICP de la GRC ou par une AC de l'ICP qui fait partie du modèle de confiance de l'ICP du gouvernement du Canada. En ce qui concerne le service Web de l'ASFC, un seul certificat de dispositif délivré spécialement à cet effet sera permis pour établir une session SSL avec le module ACE du commutateur de couche 3 de Cisco de la GRC.

- Des renseignements supplémentaires seront ajoutés aux spécifications des certificats. Ce n'est pas essentiel pour le moment, étant donné qu'un certificat approuvé par la GRC sera délivré à l'ASFC.

4.2.2 ÉTABLISSEMENT D'UNE SESSION SSL

Avant la transmission de toute transaction VER, le service Web de l'ASFC doit établir une session SSL avec le module ACE du commutateur de couche 3 de Cisco de la GRC. La liste suivante décrit les spécifications de l'interface relatives à l'établissement de la session SSL.

- Le service Web de l'ASFC crée une demande de connexion TCP/IP (synchrone);
- Le module ACE du commutateur de couche 3 de Cisco de la GRC répond à la demande (synchrone-accusé de réception);
- À la suite de l'établissement de la liaison conformément au protocole TCP, laquelle est nécessaire pour établir une connexion TCP, le service Web de l'ASFC crée la demande de session SSL;
- Le module ACE du commutateur de couche 3 de Cisco de la GRC répond au moyen d'un certificat X.509 du SSV et d'une demande d'authentification du client;
- Le service Web de l'ASFC authentifie le certificat du SSV, poursuit l'établissement de la liaison conformément au protocole SSL, puis envoie le certificat X.509;
- Le module ACE du commutateur de couche 3 de Cisco de la GRC authentifie le certificat du service Web de l'ASFC, poursuit l'établissement de la liaison conformément au protocole SSL si le certificat est authentique, puis établit une session SSL;

- La session SSL prend fin après la durée maximale approuvée par la Sous-direction de la sécurité ministérielle, ou après une période d'inactivité.

Remarque : Le SSV de la BRT est compatible avec la version 1.0 du protocole TLS.

4.2.3 TRANSACTION DE VÉRIFICATION ENTRANTE

Pour chaque demande de vérification du PDE, le service Web de l'ASFC envoie une transaction POST HTTP, ainsi qu'un paquet NIST (transaction VER) binaire chiffré selon le protocole MIME. On s'attend à ce que cette transaction POST HTTP respecte les spécifications suivantes :

- Elle sera publiée à une adresse URI (identificateur de ressource uniforme)[1];
- Elle sera transmise au moyen du protocole HTTP 1.1;
- L'en-tête HTTP doit comprendre la longueur du contenu des données chiffrées selon le protocole MIME et le type de contenu désigné comme « multipart/form data » (p. ex. « Content-Length: 912373 », « Content-Type: multipart/form-data »;
- L'en-tête HTTP doit également comprendre la disposition du contenu et le type de contenu du corps, notamment un nom de fichier unique pour chaque paquet NIST (transaction VER) transmis (p. ex. « Content-Disposition: form-data; name="attachment_field"; filename="ver1.nist" », « Content-Type: application/octet-stream »).

4.2.4 RÉPONSE SORTANTE D'UNE TRANSACTION SRV OU ERRV

Pour chaque demande de vérification du PDE qui comprend un paquet NIST (transaction VER) pouvant faire l'objet d'une interprétation, la réponse du SSV de la GRC prendra la forme d'un paquet NIST (transaction SRV ou ERRV). L'en-tête HTTP comprendra le résultat de la réponse. Si le paquet NIST (transaction VER) ne peut pas être traité en raison d'une défaillance, le SSV répondra par une erreur HTTP appropriée. La section suivante indique les spécifications des réponses qui seront renvoyées au service Web de l'ASFC :

- Chaque réponse sera exprimée sous la forme d'une réponse HTTP 1.1;
- L'en-tête HTTP comprendra la longueur du contenu des données chiffrées selon le protocole MIME et le type de contenu désigné comme « multipart/form data » (p. ex. « Content-Length: 255 », « Content-Type: multipart/form-data »);
- L'en-tête HTTP comprendra également la disposition du contenu et le type de contenu du corps, notamment un nom de fichier unique pour chaque paquet NIST de réponses (transaction SRV ou ERRV) (p. ex. « Content-Disposition: form-data; name="attachment_field"; filename="srv1.nist" », « Content-Type: application/octet-stream »);
- L'en-tête HTTP comprendra également un des en-têtes personnalisés suivants :
  - TRBVSR : <valeur> qui indique la valeur du résultat de la vérification incluse dans le paquet NIST (transaction SRV); ou
  - TRBERRCODE : <valeur> qui indique la valeur du premier code d'erreur inclus dans le paquet NIST (transaction ERRV).
- Le DCI NIST des SNP, versions 2.1.0 et 2.1.1, contient les valeurs possibles de la transaction VSR. La liste des codes d'erreur pouvant être envoyés est présentée à la prochaine section.

[1] Remarque : L'adresse URI sera fournie par la GRC.

4.2.5 ERREUR HTTP EN GUISE DE RÉPONSE

Le SSV répondra par une erreur HTTP dans le cas de toute transaction VER pour laquelle il ne peut pas répondre par une transaction SRV ou ERRV. Les erreurs HTTP pouvant être envoyées comprennent uniquement celles qui sont actuellement définies pour le protocole HTTP (p. ex. « HTTP/1.1 404 Not Found »).

5. ERREURS DE VÉRIFICATION

5.1 CODES D'ERREUR ET MESSAGES D'ERREUR

Le tableau suivant présente les codes d'erreur possibles du SSV et le message d'erreur qui y est associé.

Remarques : Le symbole % représente la valeur variable selon le champ à l'origine de l'erreur. Les sous-codes d'erreur sont destinés exclusivement à l'usage interne. Ils ne sont pas envoyés à l'ASFC. Le message d'erreur envoyé à l'ASFC est bilingue.

Code d'erreur	Sous-code d'erreur	Message d'erreur	Cause
Erreurs du service Web			
HTTP 503	S.O.	Service temporairement indisponible Aucun paquet NIST ni aucun code TRBERRCODE ne sont envoyés	La solution ACE de la BRT de la GRC ne peut pas se connecter aux serveurs Web du SSV (deux au site primaire et deux au site de reprise après sinistre). Aucun des quatre nœuds n'est donc disponible, puisque la vérification de la BRT repose sur une configuration active-active avec le site primaire et le site de reprise après sinistre, tous deux utilisés au maximum de leur capacité dans le cadre d'opérations normales.
204	S.O.	Aucune réponse pendant le délai d'attente Un paquet NIST et le code TRBERRCODE 204 sont envoyés	Le service Web s'est assuré que le paquet ne contient aucune erreur liée au Web, il a été en mesure de faire passer le paquet au processus de recherche du SSV, mais il n'a pas reçu de réponse pendant le délai d'attente de 30 secondes. Cette erreur pourrait indiquer une défaillance des services de correspondance du SSV.
400	S.O.	Paquet NIST corrompu Aucun paquet NIST n'est envoyé, mais le code TRBERRCODE 400 est envoyé	Aucun paquet n'est envoyé; le message est enregistré dans le tableau d'erreurs du SSV. Le service Web du SSV a détecté un « paquet » corrompu qui est complètement vide ou dans lequel il manque de nombreuses étiquettes essentielles.

Code d'erreur	Sous-code d'erreur	Message d'erreur	Cause
500	S.O.	Connexion refusée; canal de communication non disponible; Oracle Un paquet NIST et le code TRBERRCODE 500 sont envoyés	Le service Web s'est assuré que le paquet ne contient aucune erreur liée au Web, mais il n'a pas été en mesure de le faire passer au processus de recherche du SSV. Il n'y a pas de connexion avec le module répondant, ou la solution du SSV n'a pas pu se connecter à la base de données. Cette erreur pourrait aussi indiquer des problèmes de réseau.
Erreurs de validation du DCI NIST des SNP, version 2.1.0 (Le numéro d'étiquette est également inclus dans le message d'erreur.)			
21	7001	OBLIGATOIRE MANQUANT	Champ obligatoire manquant
21	7002	TYPE D'ENREGISTREMENT NON VALIDE %d	Type d'enregistrement non valide
21	7003	NON DÉFINI %	Champ non défini
21	7004	OCC %d > NBRE MAX OCCURRENCES %d	Excède le nombre maximal d'occurrences
21	7005	NBRE SOUS-CHAMPS %d > NBRE CFG %d	Nombre de sous-champs non valide
21	7006	TAILLE %d < TAILLE MIN %d	Longueur du champ trop faible
21	7007	TAILLE %d > TAILLE MAX %d	Longueur du champ trop élevée
21	7008	VALEUR « %.*s » N'EST PAS UN NBRE PUR	Le champ n'est pas un nombre comme attendu
21	7009	VALEUR %d < VALEUR MIN %d	La valeur numérique du champ est trop faible
21	7010	VALEUR %d > VALEUR MAX %d	La valeur numérique du champ est trop élevée
21	7011	CAR NON VAL 0x%x « %c »	Caractère non valide
21	7014	ANNÉE NON VAL : %.4s SIÈCLE NON VAL : %.2s ANNÉE NON VAL : %.2s MOIS NON VAL : %.2s	Date et heure non valides Remarque : 4 et 2 signifient 4 et 2 chiffres (p. ex. ANNÉE NON VAL : 2013).

Code d'erreur	Sous-code d'erreur	Message d'erreur	Cause
		JOUR NON VAL : %.2s HEURE NON VAL : %.2s MINUTE NON VAL : %.2s SECONDE NON VAL : %.2s FRACTION NON VAL : %.4s CAR INATTENDU : %c	
21	7015	ÉLÉMENT NON VAL : %s	Valeur de l'élément non valide
21	7016	TYPE DE TRANSACTION « %s » INCONNU	Type de transaction non valide
21	7100	IDENTIFICATEUR D'ORGANISME D'ORIGINE MANQUANT, VIDE OU NON VALIDE POUR L'ENREGISTREMENT DE TYPE 1	Le champ de l'identificateur d'organisme d'origine est vide ou manquant
21	7101	NUMÉRO DE CONTRÔLE DE TRANSACTION EN DOUBLE, MANQUANT, VIDE OU NON VALIDE POUR L'ENREGISTREMENT DE TYPE 1	Le numéro de contrôle de transaction est en double, manquant, vide ou non valide
21	7102	LE TYPE DE TRANSACTION « %1.004 » NE FIGURE PAS DANS LA LISTE CONFIGURÉE DES TYPES DE TRANSACTIONS OU LE TYPE DE TRANSACTION N'EST PAS VALIDE POUR L'ENREGISTREMENT DE TYPE 1	Type de transaction non valide
21	7103	LA DATE DOIT ÊTRE EXPRIMÉE AU FORMAT AAAAMMJJ OU IL MANQUE LA DATE DANS L'ENREGISTREMENT DE TYPE 1	Date vide, manquante ou non valide
21	7104	IDENTIFICATEUR DE SERVICE DESTINATAIRE MANQUANT, VIDE OU NON VALIDE POUR L'ENREGISTREMENT DE TYPE 1	L'identificateur de service destinataire est vide, manquant ou non valide
21	7105	VALEUR NON VALIDE « %1.011 » (RÉSOLUTION DE LECTURE INITIALE)	Résolution de lecture initiale non valide

Code d'erreur	Sous-code d'erreur	Message d'erreur	Cause
21	7106	VALEUR NON VALIDE « %1.012 » (RÉSOLUTION NOMINALE DE TRANSMISSION)	Résolution nominale de transmission non valide
Erreurs de qualité d'image			
29	29	MAUVAISE QUALITÉ (personnalisable[2])	La qualité globale des empreintes digitales n'est pas suffisante pour effectuer une vérification exacte.
30	30	IMAGES EN DOUBLE (personnalisable)	Les empreintes digitales segmentées contiennent au moins un doublon.

[2] Le texte du message d'erreur peut être modifié au moyen d'une interface utilisateur.