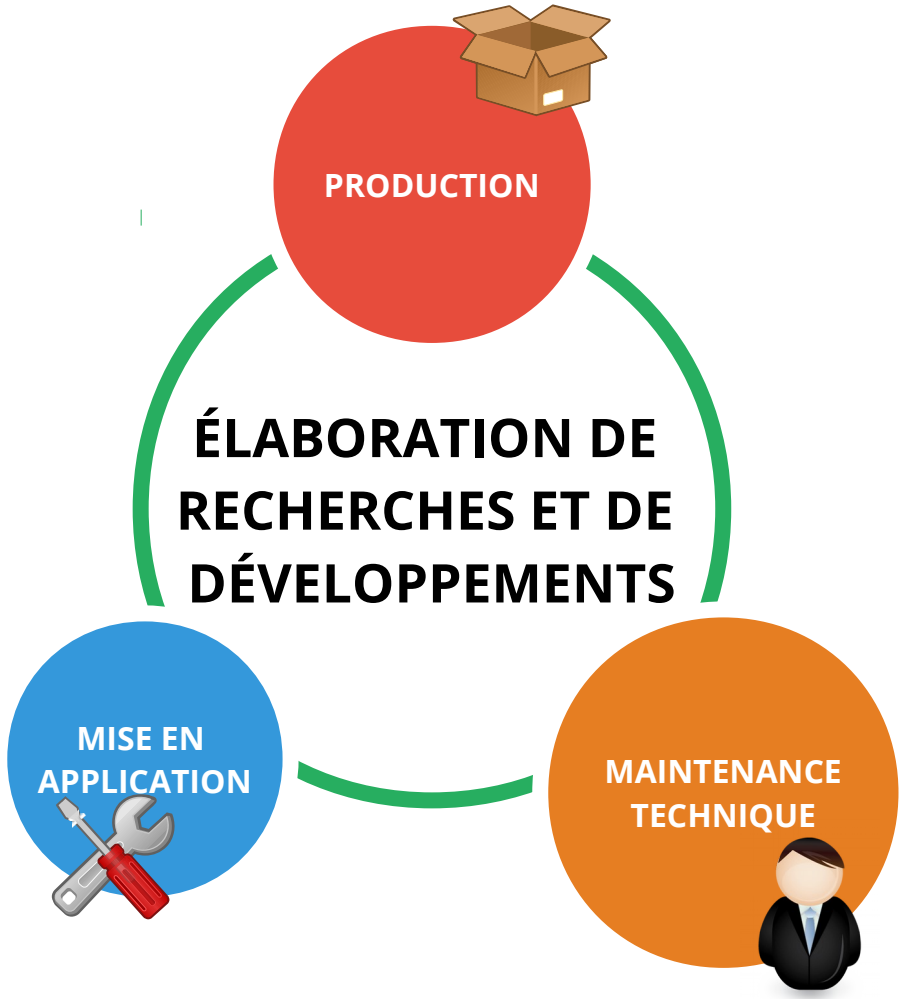
MOYENS TECHNIQUES DE LA **PROTECTION DES INFORMATIONS**

Aux réseaux de télécommunications

«BazIS»

- Le concepteur professionnel des solutions techniques de la protection des informations dans les réseaux de télécommunications;
- Fondé en 2002;
- Bureau à Moscou;
- Base personnelle de recherche et de production;
- La spécialisation consiste à la création du logiciel national protégé pour les équipements et les réseaux de communication;
- Large réseau de partenaires sur le territoire de la Fédération de Russie;

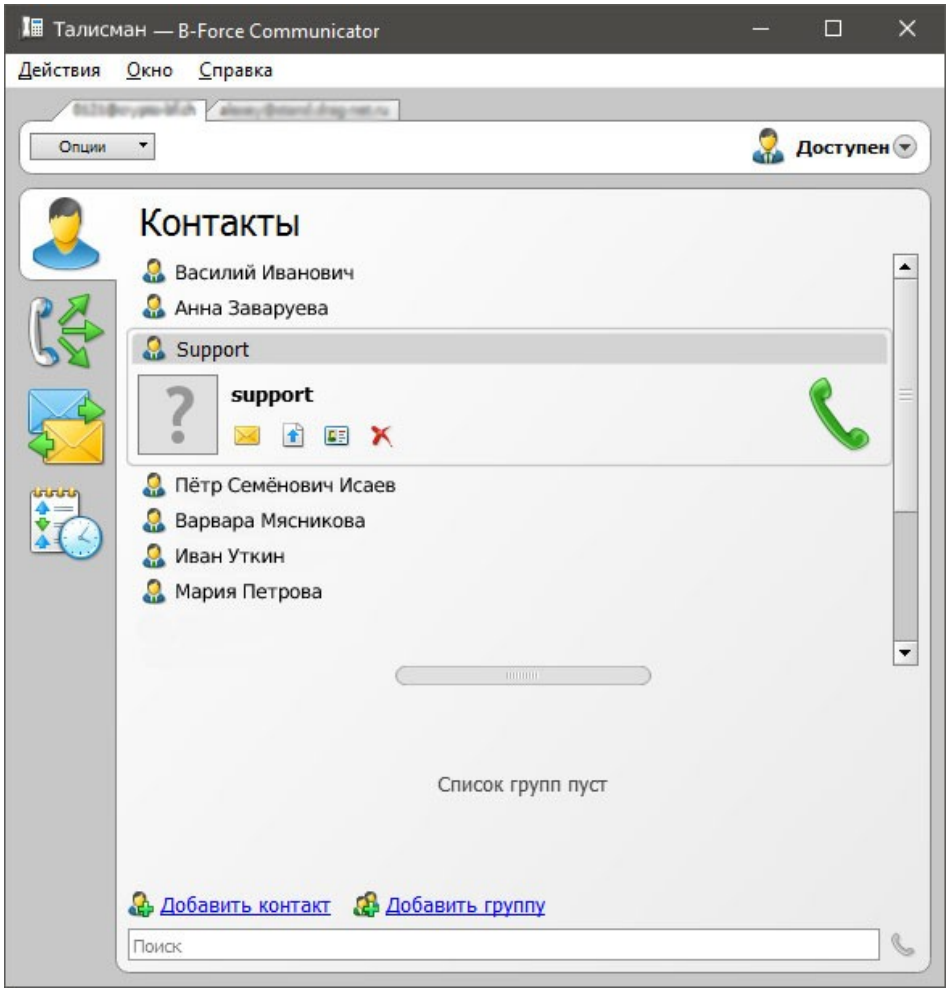


«B-Force»

Le système «B-Force» n’est pas une assurance, mais la **garantie de sécurité** de l'information durant des séances de communication. C'est une neutralisation de tous les types d’attaques contre les ressources d'information de l'abonné de la part de tout adversaire potentiel.

Le système «B-Force» utilise les algorithmes personnels et est une conception particulière innovante. L'ensemble des équipements et du logiciel remplit le plus large ensemble des fonctions de service de l'abonné associé à la qualité et à la sécurité de la communication.

«B-Force»



C’est une interface simple et claire, capable de réaliser tous les travaux de l'abonné.

«B-Force» Communication téléphonique

La téléphonie IP protégée assure entièrement les besoins de la communication. Vous pouvez réaliser les coups de téléphone sécurisés «téléphone-téléphone», «ordinateur-téléphone» ou «ordinateur-ordinateur». L'utilisation du large ensemble de codecs vocaux en fonction de la capacité de service de la voie de communication assure une haute qualité du signal vocal restitué;

«B-Force» Communication vidéo

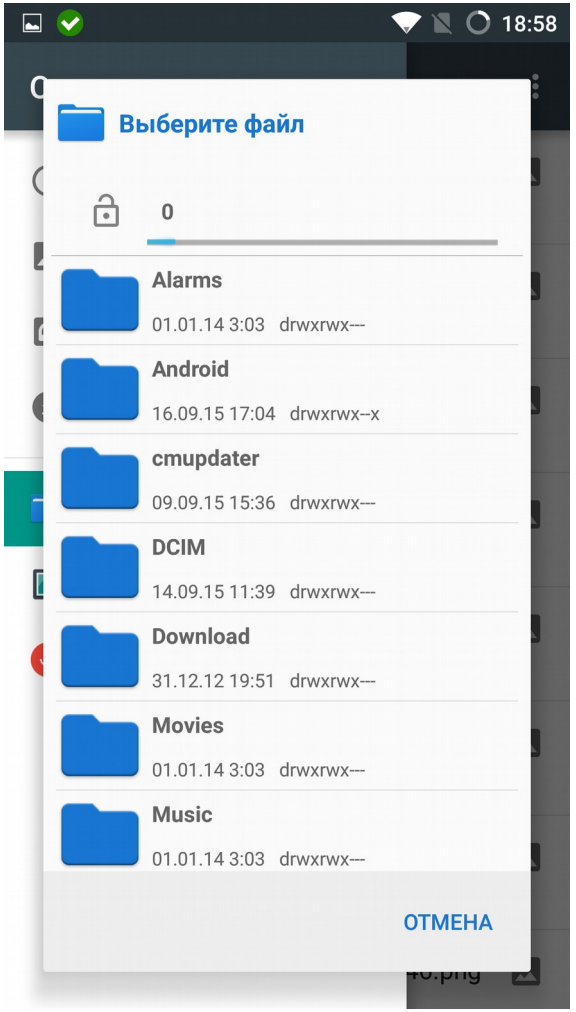
Comme les coups de téléphone simples, le communication vidéo change le niveau de communication entre les abonnés grâce à la qualité excellente du son et de l'image.

«B-Force» Messagerie

Organisation du système de la transmission des messages courts en régime (point-point), à savoir en train de la conversation avec l'abonné opposé sans destruction de communication.

«B-Force» Transfert des fichiers

Organisation du traitement protégé des documents en régime «point-point» avec l'utilisation de la signature informatique numérique conformément à GOST R 34.10-2001 à la base de valeur de la fonction hash conformément à GOST R 34.11-94 ou SHA256, SHA384 (au choix de l'abonné)



«B-Force» Courrier électronique

La lettre en régime du courrier électronique sera gardée sur le serveur avant l'apparition de l'abonné au réseau. Après cela elle sera transmise automatiquement à l'abonné. De plus si l'appareil de l'abonné est coupé ou hors de la zone de couverture du réseau le système de notification l'informera de la nécessité de la connexion au courriel par le message SMS.

«B-Force» Système de protection

Assure:

I. **Organisation** du système de chiffrement à double circuit;

- Premier circuit – «abonné-serveur»
- Deuxième circuit – «abonné-abonné»

II. **Protection** du signal d'information (vocal) contre l'identification avec la liquidation de tous les signes démasquant des séances de communication; (il y a constamment un trafic numérique «cryptogramme» dans la voie de communication et il est impossible d'établir le fait lui-même de communication des abonnés)

«B-Force» Système de protection

II.Protection contre la connexion de l'adversaire à la voie de communication; (l'indication visuelle de la ligne d'authentification de l'abonné dans la présente séance de communication fait 4 signes)

III.Protection contre la réception des informations par l'adversaire relatives aux séances précédentes de communication en cas d'une compromission (pillage) du dispositif; (les paramètres des installations de séance clés en cours sont supprimés automatiquement à la fois après la réponse de l'abonné opposé)

«B-Force» Système de protection

V.Protection contre l'apparition des voies supplémentaires de la fuite de l'information au cours du fonctionnement du dispositif; (blocage de toutes les fonctions non déclarées du smartphone à la base de l'analyse et du traitement du logiciel)

VI.Protection des informations d'adresses des abonnés (il est impossible de définir qui, quand et à qui téléphonait-il)

«B-Force» Système de protection

VII.Protection contre l'utilisation de l'appareil par l'adversaire en cas de sa compromission (perte); (blocage du dispositif compromis à distance)

VIII.Protection contre toutes les méthodes du contrôle de l'abonné du côté des télexistes GSM. (Fonctionnement sans carte SIM avec les moyens de radio coupés GSM dans les points d'accès de Wi-Fi de l'usage public)

«B-Force» Fonctions de service

I. Organisation du système de la notification de l'abonné sur la nécessité de la connexion au réseau Internet par les messages SMS, si l'appareil de l'abonné est coupé ou est hors de la zone de couverture du réseau;

II. Organisation du système de recherche de l'abonné par les numéros préétablis sur les réseaux de transmission ouverts PSTN et GSM;

«B-Force» Fonctions de service

III.Possibilité du complément (élimination) des abonnés du groupe à distance;

IV.Connexion instantanée sans numérotation;

V. Sauvegarde de toutes les fonctions principales de service du modèle de base de l'appareil;

«B-Force» Termes et définitions

RTP *(Real-time Transport Protocol)* — fonctionne au niveau de transport et est utilisé à la transmission du trafic en temps réel;

TLS *(Transport Layer Security)* — procès-verbal cryptographique assurant la transmission protégée de données entre les noeuds au réseau Internet;

SRTP *(Secure Real-time Transport Protocol)* — le procès-verbal sécurisé de la transmission de données en temps réel qui est destiné au chiffrement, à l'échange de clés d'après l'algorithme de Diffie-Hellman, à l'authentification du message, à l'intégrité, à la protection contre le remplacement des données RTP aux transmissions medias et aux applications unidirectionnelles et multicast;

«B-Force» Termes et définitions

DMZ *(Multi-Service Access Node)* — technologie de la protection des serveurs, croisant le périmètre;

SIP *(Session Initiation Protocol — procès-verbal de l'établissement de la séance*) — le standard du moyen de l'établissement et de l'achèvement de la séance Internet d'utilisateur insérant l'échange du contenu multimédia (vidéo- et audioconférences, messages instantanés);

SIP proksi-serveur *(proxy — «représentant»*) présente les intérêts de l'utilisateur au réseau. Il accepte les demandes et les traite;

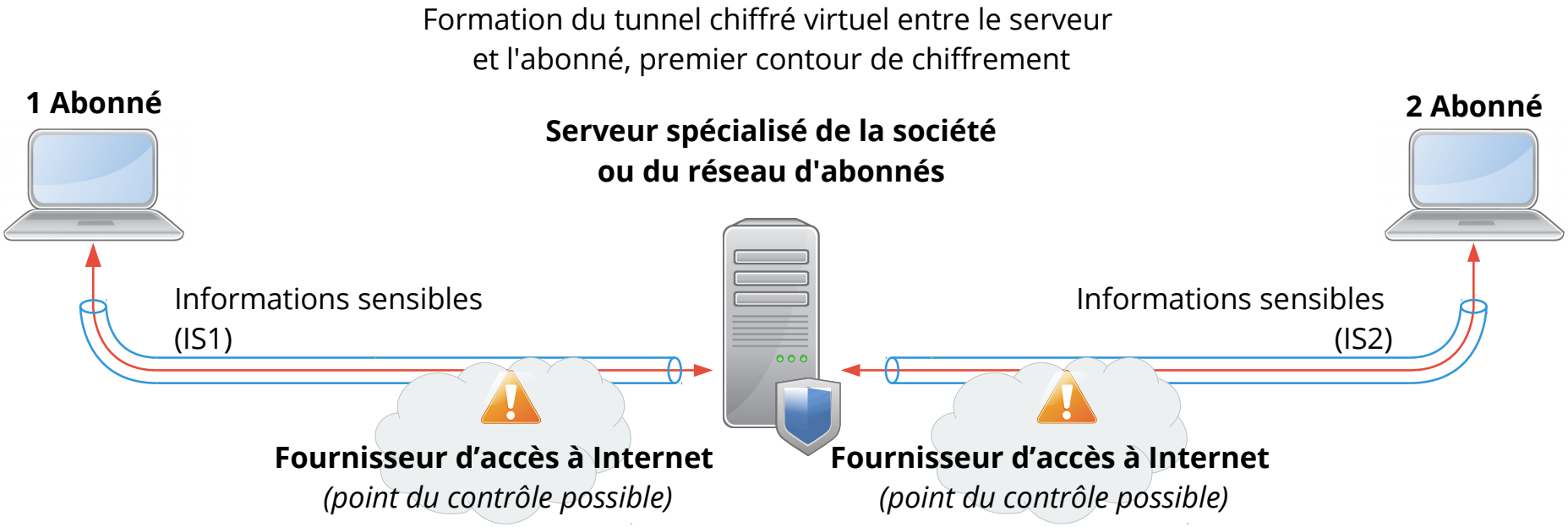
CLI *(Call Level Interface)* — Interface du niveau des appels. Le standard de logiciel fixé au document ISO/IEC 9075-3:2003.

«B-Force» Modes

Passage des signaux ouverts d'information en régime
«établissement de connexion avec le serveur spécialisé»

- L'enregistrement de l'abonné au réseau se fait automatiquement à la connexion de l'ordinateur sans participation de l'abonné;
- Établissement de connexion;
- Formation du tunnel chiffré virtuel entre le serveur et l'abonné;

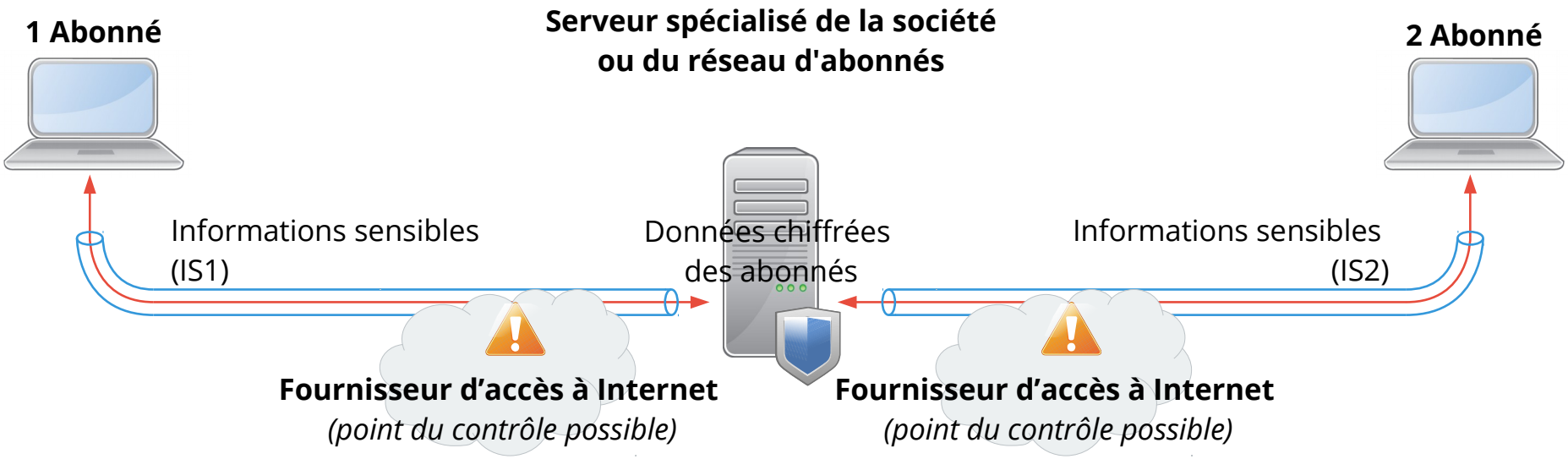
«B-Force» Modes



- Chiffrement des donnés d'identification des abonnés;
- Chiffrement de l'information d'adresses, à savoir, il est impossible de définir qui, quand à qui téléphonait-il;
- Chiffrement des informations sous régime du «courrier électronique»;

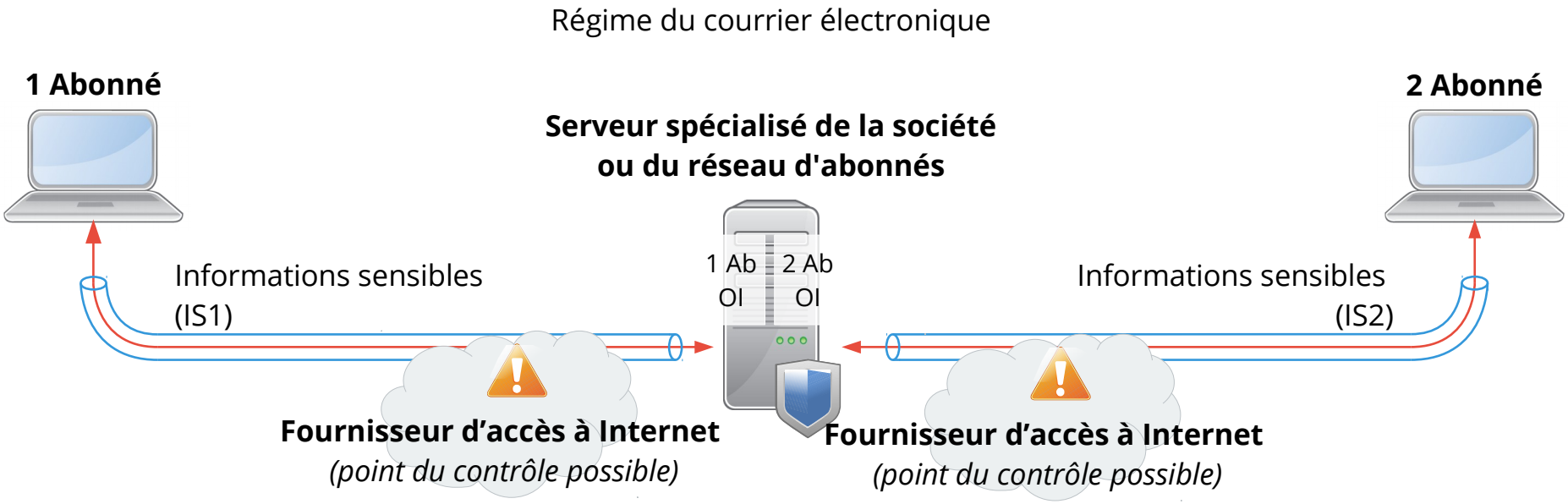
«B-Force» Modes

Enregistrement des abonnés au réseau de télécommunications



- Toutes les données nécessaires d'enregistrement des abonnés sont gardées sur le serveur sous une forme chiffrée. Les systèmes de protection ne permettent pas de les recevoir même si l'équipement se trouve dans les mains de l'adversaire. Le serveur fonctionne sous gestion du système d'exploitation DNLinux spécialement élaboré.

«B-Force» Modes

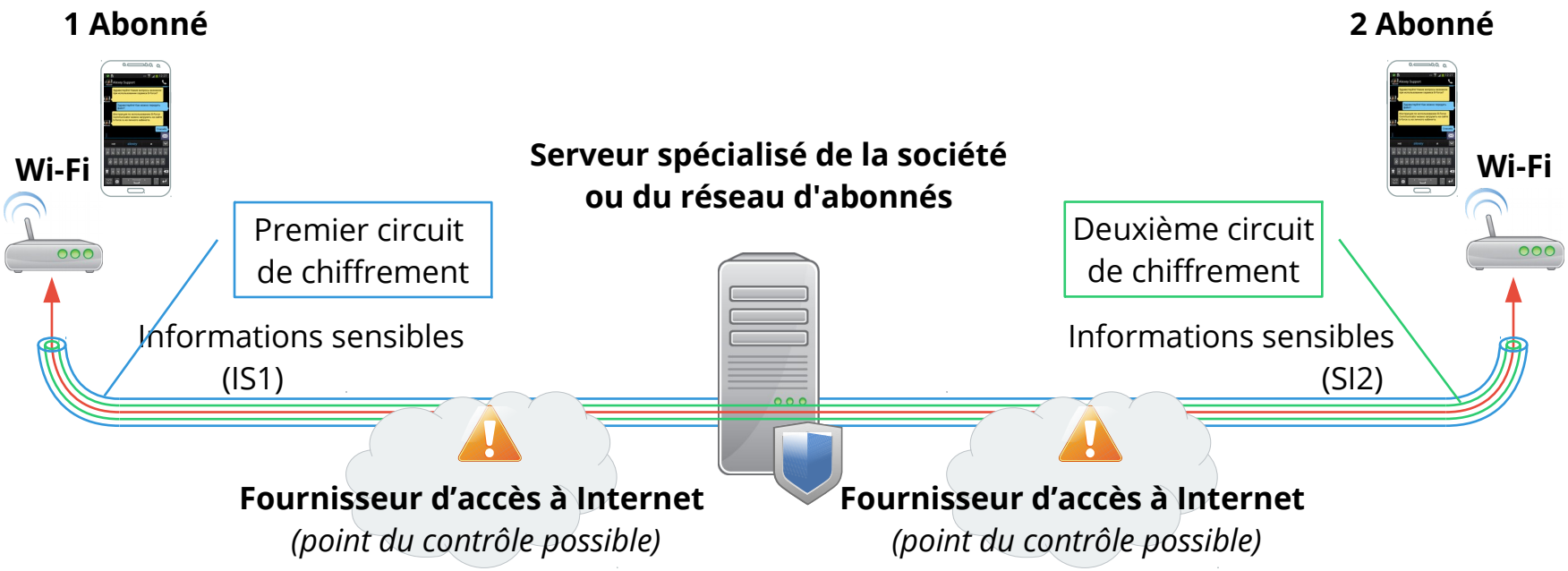


- Ce régime est utilisé pour transmettre des fichiers et des messages courts en absence du destinataire au réseau de télécommunications. Le message est transmis par la voie de communication chiffrée au serveur, où il est gardé sous forme ouverte avant l'apparition du destinataire au réseau. Après cela il est chiffré et transmis automatiquement à l'abonné.

«B-Force» Modes

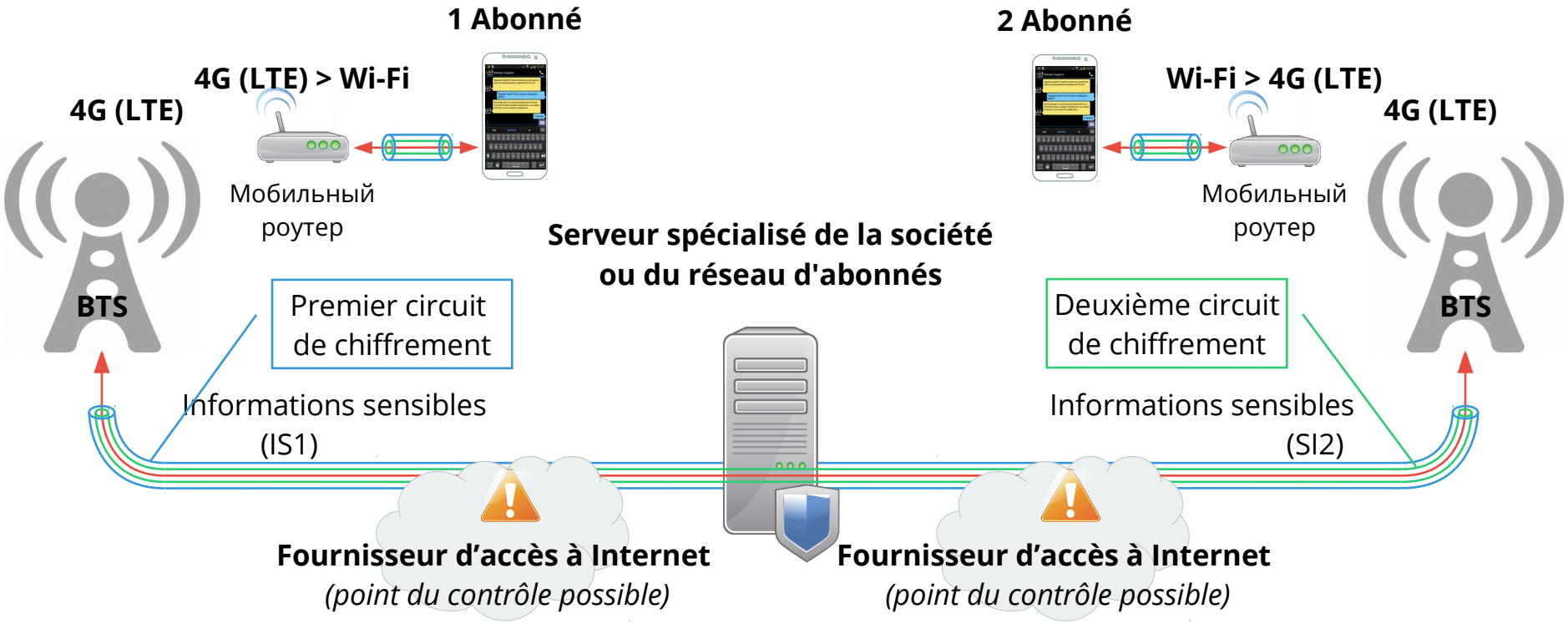
- Ce régime assure le plus haut niveau de la sécurité de l'information. À la connexion (abonné-abonné) le deuxième circuit est formé à l'intérieur du premier circuit de chiffrement, où le serveur ne participe pas déjà. Les informations sont chiffrées deux fois par de différents algorithmes. Le procès de formation des clés de séance du deuxième circuit de chiffrement passe sous la protection du premier et l'adversaire ne le voit pas.

«B-Force» Modes



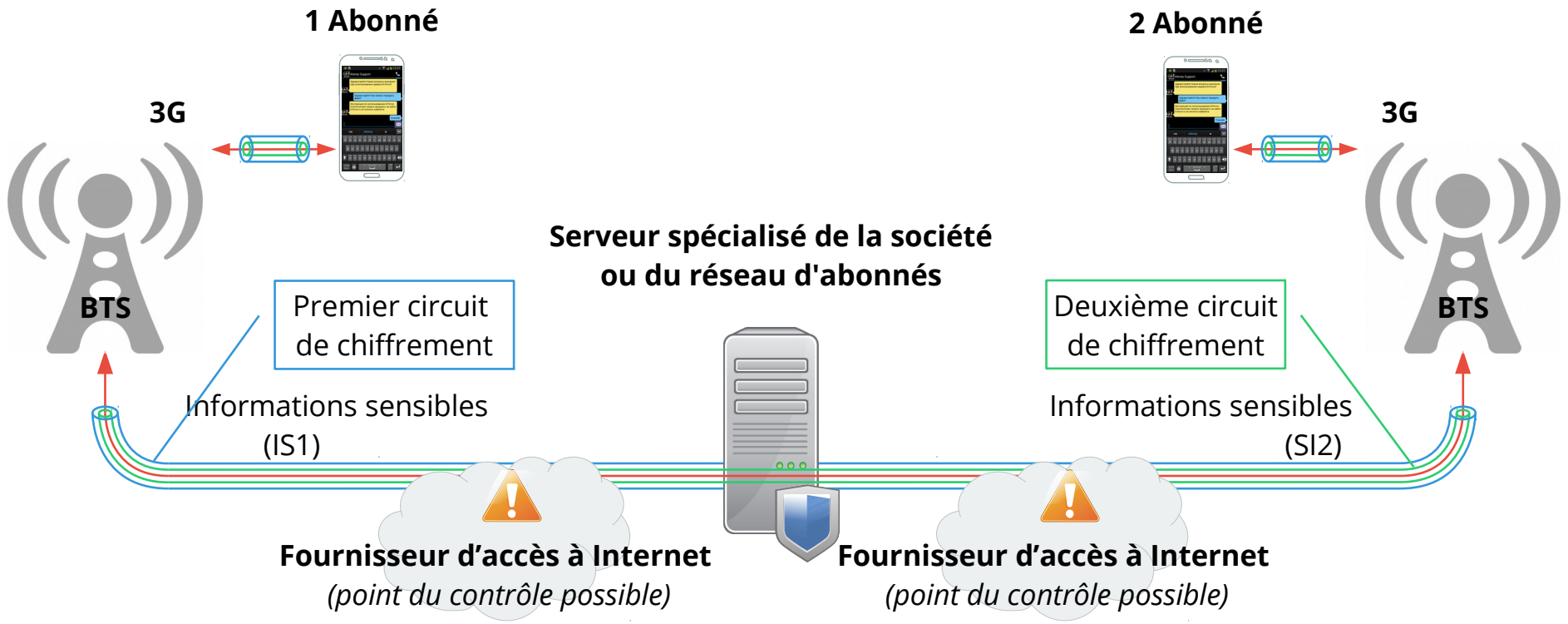
- À l'utilisation de cette variante du système l'adversaire ne pourra même définir l'emplacement des abonnés, puisque les points d'accès peuvent être particuliers. La séance de connexion est organisée sans carte SIM avec les moyens de radio coupés GSM.

«B-Force» Modes



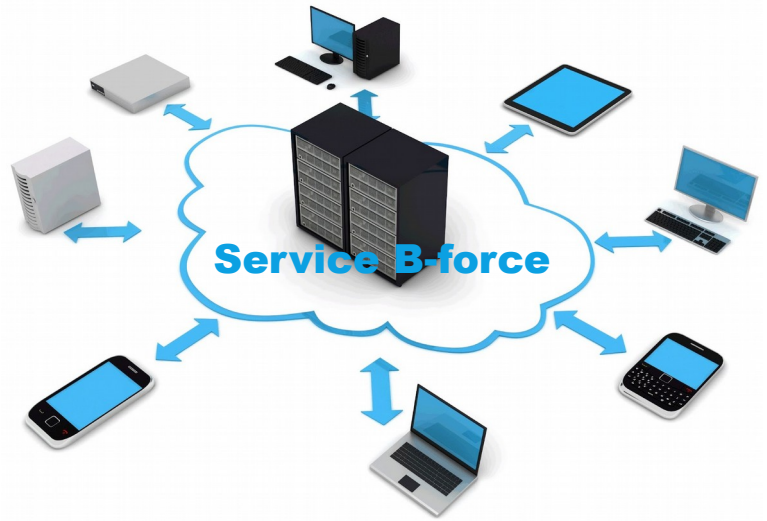
- Variante de la constitution du système avec l'utilisation du routeur mobile 4G (LTE)

«B-Force» Modes



- Fonctionnement par les canaux 3G

«B-Force» Architecture du réseau



- Le système »B-Force» utilise les procès-verbaux standard ouverts : SIP, TLS, SRTP, ZRTP.
- Le TLS présente une voie chiffrée authentique pour la transmission du système d'alarme, le SRTP assure le chiffrement et l'authentification du trafic média, le ZRTP réalise l'échange de clés pour l'assurance de communication «point-point». Le soutien du schéma SIPS prévoit l'installation d'une connexion chiffrée TLS sur tous les segments du réseau de la transmission de données du coup de téléphone. L'ensemble de tous ces procès-verbaux permet de dire de l'assurance de sécurité de l'information transmise.

«B-Force» Exigences à la voie de communication

Le système exige la connexion constante à Internet. De divers modes de connexion ont de diverses exigences minimales à la voie de communication. Le tableau ci-dessous fournit la capacité de fonctionnement de tous les types de connexion affectés par l'application, en fonction de la voie d'accès accessible au réseau Internet.

Type de communication	LTE / Wi-Fi	3G	GPRS / EDGE
Rappels vidéo	+	-	-
Transmission du fichier	+	+	-
Communication vocale	+	+	-
Message	+	+	+
Statut de l'abonné	+	+	+