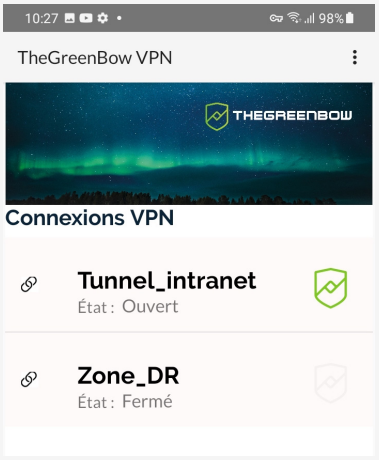
CLIENT VPN ANDROID

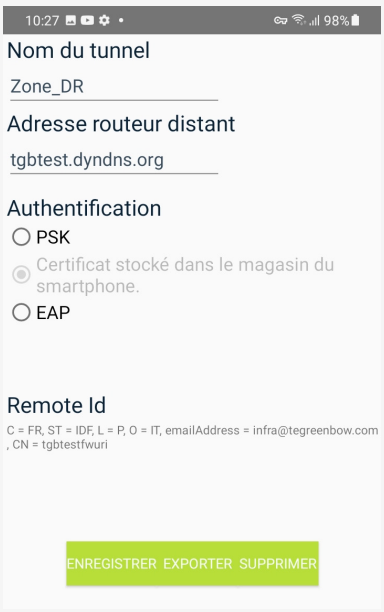
Le client VPN de confiance pour vos connexions mobiles

Le Client VPN Android sécurise les échanges de données depuis et vers les smartphones et les tablettes. Particulièrement adapté à la gestion des systèmes industriels (maintenance, diagnostics, logistique...), il répond également aux exigences de protection des communications critiques pour les services de sécurité publics et privés.



Haut niveau de sécurité

Le Client VPN Android a été développé en suivant les recommandations du NIST et de l'ANSSI. Dans sa version actuelle, il est capable de répondre au profil IPsec DR (Diffusion Restreinte) d'un point de vue protocolaire. Il est donc compatible avec le référentiel IPsec DR de l'ANSSI.
L'ensemble des protocoles et algorithmes mis en œuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN IPsec et OpenVPN du marché, qu'elles soient logicielles ou matérielles, y compris celles qui prennent en charge le référentiel IPsec DR.



Facilité d'installation

L'installation sur n'importe quel terminal Android s'effectue de manière transparente pour l'utilisateur. Le logiciel prend en charge une variété de protocoles, de paramètres et d'options permettant une interopérabilité avec votre passerelle / pare-feu et votre PKI.
Le Client VPN Android peut désormais accéder aux certificats stockés dans le magasin de certificats Android, ce qui contribue à simplifier encore davantage l'installation.

Simplicité d'utilisation

Le Client VPN Android simplifie l'usage du VPN en proposant une interface utilisateur ergonomique pour établir des connexions sécurisées vers votre système d'information.
Les utilisateurs ont une vision directe de l'état des connexions VPN pour vérifier que leurs communications sont bien protégées. Ils peuvent également se reposer sur la fonction VPN permanent pour garder l'esprit tranquille avec la certitude que la protection est maintenue sans aucune intervention de leur part.

CARACTÉRISTIQUES TECHNIQUES

Protocoles	• IPsec IKEv2 • OpenVPN • Réseau : IPv4, NAT-Traversal, fragmentation IKE
Authentification	• Authentification : EAP, PSK, certificats, Extra Auth, Multiple Auth • Gestion des certificats X.509 : PKCS#12, PFX
Cryptographie	• DH 14-21 & 28, AES 128/196/256 SHA-2 (256/384/512) • Méthodes d'authentification des certificats : Méthode 1 : RSA Digital Signature avec SHA-2 [RFC 7296] Méthodes 9-11 : ECDSA « secp » avec SHA-2 [RFC 4754] Méthode 14 : RSASSA-PKCS1-v1_5, RSASSA-PSS [RFC 7427] Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2
Configuration requise	• Android 10 ou supérieur • 40 Mo d'espace disponible pour l'application et les données

Principales fonctionnalités

- Compatible avec les passerelles qui prennent en charge le référentiel IPsec DR
- Importation de certificats stockés dans le magasin de certificats Android
- Activation permanente du VPN, y compris lorsque le client n'est pas lancé
- Activation des licences par TAS (manuelle ou dans le tunnel)
- Nouvelle interface graphique
- Vérification des CA de la passerelle
- Gestion des tunnels : full tunneling, split tunneling
- Continuité de service : DPD (Dead Peer Detection), passerelle redondante
- Obtention des paramètres réseau depuis la passerelle (mode CP)
- Configuration et établissement de connexion SSL (OpenVPN)
- Fin de prise en charge de IKEv1

THEGREENBOW

TheGreenBow – 28 rue Caumartin, 75009 Paris, France – sales@thegreenbow.com – +33 1 43 12 39 37
www.thegreenbow.com