Annexe 1 – Govroam Technical Policy

1. Procédure d'activation

Le(s) serveur(s) d'authentification de l' "govroam identity provider" doi(ven)t être accessible(s) à partir des serveurs mandataires ("proxies") RADIUS de BELNET à des fins d'authentification et de gestion des comptes.

L' "identity provider" doit créer un compte test govroam (nom d'utilisateur et mot de passe govroam) qui sera rendu accessible pour l'assistance lors du test de la pré-connexion, de la surveillance continue, des activités de support et de la détection des incidents. En cas de changement du mot de passe du compte test, BELNET doit être informé par la "home organization" en temps utile.

Le "govroam resource provider" peut offrir tout support ; toutefois, le réseau LAN IEEE 802.11b sans fil est au minimum requis bien que le 802.11g soit également recommandé.

Le "govroam resource provider" doit déployer le SSID "govroam" et la procédure d'authentification IEEE 802.1X "Extensible Authentification Protocol" (EAP) (hormis EAP-MD5) pour promouvoir un service cohérent et un niveau de sécurité minimum. Le SSID govroam devrait être diffusé.

Le "govroam resource provider" doit au minimum implémenter la norme IEEE 802.1X et le protocole WPA/TKIP, ou des versions supérieures. Il est vivement recommandé d'implémenter le protocole WPA2/AES.

Le "govroam resource provider" doit au moins offrir :
- Standard IPSec VPN : IP protocols 50 (ESP) and 51 (AH) egress; UDP/500 (IKE) egress only
- OpenVPN 2.0 : UDP/1194
- IPsec NAT-Traversal UDP/4500
- Cisco IPSec VPN over TCP : TCP/10000 egress only
- PPTP VPN : IP protocol 47 (GRE) ingress and egress; TCP/1723 egress
- SSH : TCP/22 egress only
- HTTP : TCP/80 egress only
- HTTPS : TCP/443 egress only
- IMAP2+4 : TCP/143 egress only
- IMAP3 : TCP/220 egress only
- IMAPS : TCP/993 egress only
- POP : TCP/110 egress only
- POP3S : TCP/995 egress only
- Passive (S)FTP : TCP/21 egress only
- SMTPS : TCP/465 egress only
- SMTP submit with STARTTLS : TCP/587 egress only
- RDP : TCP/3389 egress only

Le "govroam resource provider" devrait offrir :

• Standard IPSec VPN : IP protocols 50 (ESP) and 51 (AH) ingress
• IPv6 Tunnel Broker service : IP protocol 41 ingress and egress

Le "govroam resource provider" devrait mettre en place un réseau local virtuel (VLAN) visiteur pour les utilisateurs govroam authentifiés, lequel ne doit pas être partagé avec d'autres services de réseau.

2. Identification

Les "govroam identity providers" doivent enregistrer toutes les demandes d'authentification et de comptabilisation ; les informations suivantes doivent être enregistrées :

1. la date et l'heure de réception de la demande d'authentification
2. l'identifiant de la demande RADIUS
3. le résultat de l'authentification renvoyée par la base de données d'authentification
4. le motif donné en cas de refus ou d'échec de l'authentification
5. la valeur du type de statut de comptabilisation.

Le "govroam identity provider" doit tenir un registre de toutes les demandes d'authentification et de comptabilisation pendant au minimum douze mois et au maximum vingt-quatre mois. La coopération concernant le contenu de ces registres est limitée aux utilisateurs govroam enregistrés et à la personne de contact technique de BELNET pour fournir une assistance dans le cadre de la résolution de problèmes spécifiques de sécurité ou d'abus rapportés à BELNET.

Le "govroam resource provider" doit enregistrer toutes les transactions DHCP, y compris :

1. la date et l'heure de délivrance du bail DHCP du client
2. l'adresse MAC du client
3. l'adresse IP attribuée au client.

Le "govroam resource provider" doit tenir un registre des transactions DHCP pendant au minimum douze mois et au maximum vingt-quatre mois. La coopération concernant le contenu de ces registres est limitée aux utilisateurs govroam enregistrés et à la personne de contact technique de BELNET pour fournir une assistance dans le cadre de la résolution de problèmes spécifiques de sécurité ou d'abus rapportés à BELNET.

Le "govroam resource provider" ne doit enregistrer aucun mot de passe.

3. Assistance et conseils aux utilisateurs govroam

L' "identity provider" doit fournir assistance aux utilisateurs qui sollicitent un accès auprès d'un "govroam resource provider".

Le "govroam resource provider" doit fournir assistance aux utilisateurs d'autres "govroam identity providers" qui demandent des services govroam sur le campus de leur "govroam identity provider".

Le "govroam resource provider" doit publier les informations locales relatives aux services govroam sur les pages internet y consacrées du site internet de leur organisation, lesquelles contiennent au moins les informations suivantes :

1. un texte (comprenant notamment un lien url) qui confirme l'adhésion à la présente police (document publié sur le site http://www.govroam.be)
2. un lien hypertexte vers un site internet donnant accès à la police d'utilisation acceptable de le "govroam resource provider" ou un équivalent
3. une liste ou une carte représentant les zones couvertes par un accès govroam
4. les détails de la diffusion ou de la non-diffusion du système SSID comme govroam
5. les détails de la procédure d'authentification et des services offerts autorisés
6. les détails de l'utilisation d'un serveur mandataire non transparent incluant les instructions de configuration de l'utilisateur (le cas échéant)
7. un lien hypertexte vers le site internet http://www.govroam.be et l'affichage du logo govroam et de la déclaration de la marque déposée
8. dans le cas où l'activité de l'utilisateur est surveillée, le "govroam resource provider" doit clairement le signaler, y compris la méthode de surveillance de manière à se conformer à la législation nationale, y compris la durée de rétention des informations et les personnes y ayant accès
9. les coordonnées du service d'assistance technique approprié qui est responsable des services govroam.

4. Glossaire des acronymes

Dans le cadre de la mise en place et de l'exécution du service, les acronymes utilisés auront la signification suivante :

AH :	Authentication Header
AUP :	Acceptable Usage Policy
CERT :	Computer Emergency Response Team
DHCP :	Dynamic Host Configuration Protocol
EAP :	Extensible Authentication Protocol
Govroam :	Government Roaming
ESP :	Encapsulating Security Payload
FTP :	File Transfer Protocol
GRE :	Generic Routing Encapsulation
HTTP :	Hypertext Transfer Protocol
HTTPS :	Secured HTTP

IEEE :	Institute of Electrical and Electronics Engineers
IKE :	Internet Key Exchange
IMAP :	Internet Message Access Protocol
IMAPS :	Secured IMAP
IP :	Internet Protocol
IPSec :	IP Secured
LAN :	Local Area Network
MAC :	Media Access Control
MD5 :	Message Digest algorithm (version 5)
NAT :	Network Address Translation
POP3 :	Post Office Protocol
PPTP :	Point to Point Tunneling Protocol
RADIUS :	Remote Authentication Dial In User Service
RDP :	Remote Desktop Protocol
RFC :	Request For Comments
SMTP :	Simple Mail Transfer Protocol
SMTPS :	Secured SMTP
SSH :	Secured Shell
SSID :	Service Set Identifier
TCP :	Transmission Control Protocol
TERENA :	Trans European Research and Education Networking Association
TKIP :	Temporal Key Integrity Protocol
TLS :	Transport Layer Security
TTLS :	Tunneled TLS
UDP :	User Datagram Protocol
VLAN :	Virtual LAN
VPN :	Virtual Private Network
WEP :	Wired Equivalent Privacy
Wifi :	Wireless Fidelity
WPA :	Wifi Protected Access