Bijlage 1 - Govroam Technical Policy

1. Activeringsprocedure

De authenticatieserver(s) van de govroam identity provider moet(en) vanuit de BELNET RADIUS proxies bereikbaar zijn met het oog op authenticatie en account beheer.

De identity provider moet een govroam test account (govroam gebruikersnaam en wachtwoord) aanmaken, die beschikbaar wordt gesteld voor bijstand bij pre-connection-testing, doorlopend toezicht, ondersteuning en bij activiteiten betreffende het zoeken naar defecten. Indien het wachtwoord van de testaccount wordt gewijzigd, moet BELNET daarvan tijdig op de hoogte worden gebracht door de home organization.

De govroam resource provider mag om het even welke media aanbieden; als minimum is echter wireless LAN IEEE 802.11b vereist, terwijl 802,11g eveneens aanbevolen is.

De govroam resource provider moet de SSID 'govroam' en IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (met uitsluiting van EAP-MD5) inzetten ter bevordering van een constante dienst en een minimaal veiligheidsniveau, De SSID govroam zou moeten worden uitgezonden.

De govroam resource provider moet tenminste IEEE 802.1X en WPA/TKIP, of beter, implementeren. Het is streng aanbevolen om WPA2/AES te implementeren.

De resource provider van govroam moet tenminste wat volgt aanbieden:
- Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) egress; UDP/500 (IKE) egress only
- OpenVPN 2.0: UDP/1194
- IPsec NATTraversal 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

The govroam resource provider should offer:
- Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) ingress

• IPv6 Tunnel Broker service: IP protocol 41 ingress and egress

De govroam resource provider moet een visitor virtual local area network (VLAN) implementeren voor govroam geauthenticeerde gebruikers dat niet mag worden gedeeld met andere netwerkdiensten.

2. Logging

Govroam identity providers moeten alle authenticatieverzoeken en accountingverzoeken registreren; de volgende informatie moet worden opgeslagen:

1. de datum en het tijdstip van ontvangst van het authenticatieverzoek
2. de RADIUS request's identifier
3. het resultaat van de authenticatie dat door de authenticatiegegevensbank wordt teruggestuurd
4. de opgegeven reden indien de authenticatie wordt geweigerd of is mislukt
5. de waarde van het accounting statustype van het verzoek.

De govroam identity provider moet gedurende minimum twaalf maanden en maximum vierentwintig maanden een register bijhouden van alle authenticatie-en accountingverzoeken. Samenwerking inzake de inhoud van deze registers zal beperkt worden tot geregistreerde govroam gebruikers en de BELNET technisch contactpersoon voor bijstand bij de oplossing van specifieke veiligheids- of misbruikkwesties die aan BELNET werden gerapporteerd.

De govroam resource provider moet alle DHCP-transacties registreren, met inbegrip van:

1. de datum en het tijdstip van uitgifte van de DHCP lease van de klant
2. het MAC adres van de klant
3. het IP-adres dat aan de klant wordt toegekend.

De govroam resource provider moet gedurende minimum twaalf maanden en maximum vierentwintig maanden een register bijhouden van de DHCP transacties. Samenwerking inzake de inhoud van deze registers is beperkt tot geregistreerde govroam gebruikers en BELNET ondersteuningsdiensten voor bijstand bij de oplossing van specifieke bijzondere veiligheids- of misbruikkwesties die aan BELNET werden gerapporteerd.

De govroam resource provider mag geen wachtwoorden registreren.

3. Govroam gebruikersondersteuning en –begeleiding

De identity provider moet ondersteuning verstrekken aan zijn gebruikers die toegang vragen tot een govroam resource provider.

De govroam resource provider moet ondersteuning verstrekken aan gebruikers van andere govroam identity provider die om govroam diensten verzoeken bij hun campus die de govroam identity provider is.

De govroam resource provider moet plaatselijke informatie publiceren inzake govroam diensten op speciaal daartoe bestemde pagina's op de website van de instelling. Deze pagina's moeten de volgende minimuminformatie bevatten:

1. een tekst (met inbegrip van een url link) die de aanvaarding bevestigt van deze policy (document gepubliceerd op www.govroam.be)
2. een hyperlink naar een website naar het beleid van govroam acceptable use policy, van de resource provider, of gelijkwaardigeen lijst of plan met vermelding van de gebieden van dekking van govroam toegangde details van de broadcast of non-broadcast SSID van govroam.
3. details van het authenticatie-proces en aangeboden toegelaten dienstendetails inzake het gebruik van een nontransparent application proxy met inbegrip van configuratierichtlijnen voor de gebruiker (indien toepasselijk)
4. een hyperlink naar de website http://www.govroam.be en het posten van het govroam logo en de trademark statement (merkverklaring)
5. als de activiteiten van de gebruiker worden gecontroleerd, moet de govroam resource provider dat uitdrukkelijk meedelen, met inbegrip van de wijze van controle met het oog op naleving van de nationale wettelijke regelingen, met inbegrip van hoe lang de informatie wordt bewaard en wie er toegang tot heeft
6. de contactgegevens van de technische support die verantwoordelijk is voor govroam diensten.

4. Acroniemen

In het kader van de installatie en de uitvoering van de dienst, zullen de gebruikte acroniemen de volgende betekenis hebben:

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 Acces