secusmart | BlackBerry Subsidiary

SecuSUITE for Government

Tap-proof Communication for International Governments

Secusmart's software-based encryption solution provides tap-proof intra-governmental communication

SecuSUITE for Government

- Cross platform (available for iOS, Android, BlackBerry)
- NIAP PP compliant
- Option to use Smartcard based Hardware token
- On premise installation of the system provides full sovereignty and control of the customer
- Solution works globally, accommodating all carriers and bearers
- Instantaneous call setup with ultra fast key agreement and superb voice quality

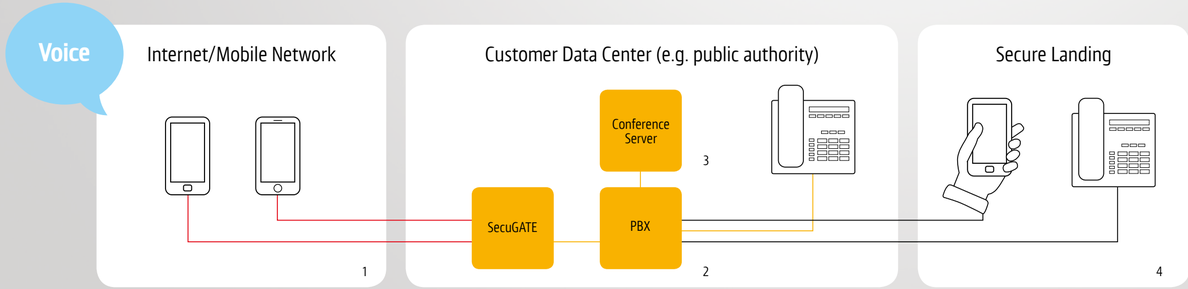
Certifications and approvals section

NIAP Certification
- VoIP Clients for iOS, Android and BlackBerry 10 are being certified according to NIAP PP for Mobile VoIP
- iPhone 6, Samsung Galaxy S7 and BlackBerry 10.3.3 are being certified according to NIAP PP MD
- SIP Server is being certified according to NIAP PP for SIP Server & Network Devices
- Certification Scheme & Timeline:
  → Expecting CSfC "under evaluation listing" (NIAP) for Q4 2016

Approval for Government of Canada for 'Secret' use under the SPfC program
- Performing Technical Proof-of-Service (T-PoS) with Shared Services Canada (SSC)
- Expecting Government of Canada approval for 'GC Secret' use to be awarded turn of the year 2016/2017 for Smartphone for Classified (SPfC)

Compliance with NSA MACP
- Solution is designed to meet the requirements of MACP
  → 2 independent layers of cryptography for protection of DAR- and Data-in-Transit
  → Outer layer of Data-in-Transit encryption can be configured as IPSec VPN with Suite B compliant cipher suite

Overview use cases



Further explanations of possible use cases

1) End to end secure mobile calls
   → Both participants are equipped with SecuSUITE and registered on the SecuGATE. The call is end to end encrypted
2) Break out calls to fixed net telephones in the corresponding agency
   → Call is encrypted between the secure mobile device and the SecuGATE. SecuGATE decrypts the call and routes it via a SIP trunk to the PBX. Vice versa from the extension to the secure mobile is possible, too (by dialing a defined Prefix)
3) Break out calls to a conference server
   → Call is encrypted between the secure mobile device and the SecuGATE. SecuGATE decrypts the call and routes it via a SIP trunk to the PBX and to the conference server
4) "secure landing": break out calls to any other device outside of the customer organization
   → Call is encrypted between the secure mobile device and the SecuGATE. SecuGATE decrypts the call and routes it via a SIP trunk to the PBX. Second part of the call between PBX and any other PSTN device is unencrypted.

secusmart | BlackBerry Subsidiary

Would you like to find out more about our security solutions?
Just give us a call or send us an E-Mail to arrange a personal consultation.

BlackBerry Limited
1776 Wilson Boulevard
Arlington, VA 22209 – 2504

Contacts:
Matthew Landa
Director Government Sales, Civilian
malanda@blackberry.com
+1 202.706.0817

William Witten
Director Government Sales, DoD
wwitten@blackberry.com
+1 202.355.5012