




Cellcrypt[®] FEDERAL



WALANG PAGTITIWALA
MGA LIGTAS NA KOMUNIKASYON
& DATA-IN-TRANSIT



A photograph of soldiers in a desert environment. In the foreground, a soldier in full combat gear, including a helmet and sunglasses, is looking towards the right. In the background, a helicopter is flying over a gravelly area, and other soldiers are visible. The scene is set in a dry, open landscape under a clear blue sky.

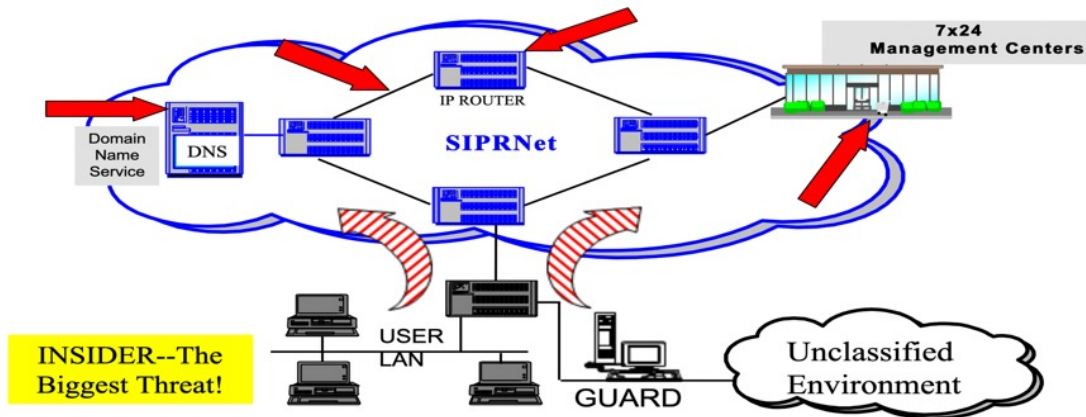
Magtiwala sa isang walang katiyakan na mundo

- Buong katiyakan para sa Komunikasyon at Data-in-Transit
- Kahit na sa mahigpit, walang katiyakan na kapaligiran na maagap na nakompromiso



SIPRNet Security Risks

The Threat Methods: **Physical** & **Electronic**
 Targets: **Hosts, Enclaves, Networks**



Walled Garden

Pag-asa sa isang

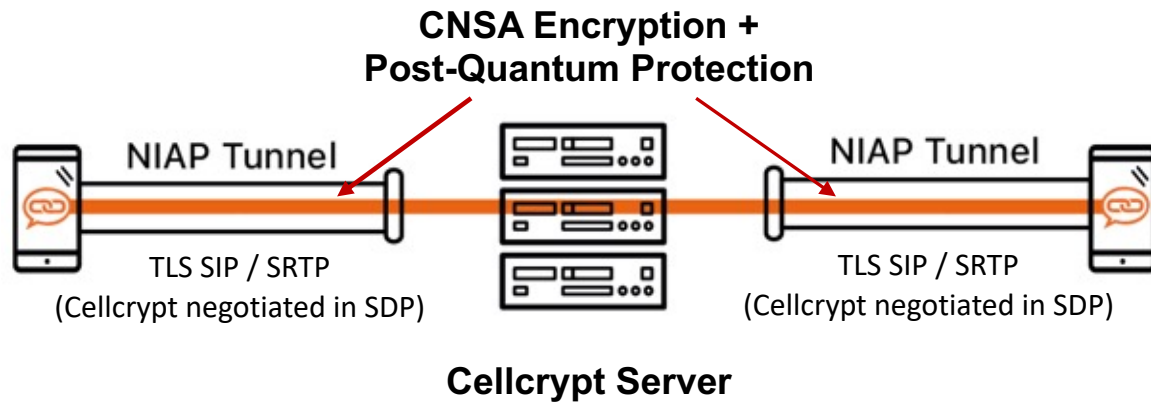
Mapagkakatiwalaang Network

- Maraming solusyon ang umaasa sa ‘tiwala’ sa isang “Walled Garden” ibig sabihin, mga kumpanyang nagbibigay ng solusyon, mga indibidwal na nagpapatakbo ng sistema at seguridad ng network
- Ang Walled Gardens ay mahina laban sa ilang mga banta at hindi nila tinatalakay ang pinakamalaking problema – ang INSIDER – ang pinakamalaking banta gaya ng kinikilala ng DISA

Harvest Now, Decrypt Later

Ang banta sa Quantum Computing

- Bagama't ang mga kuwantum kompyuter ay sapat na makapangyarihan upang sirain ang pinakamalakas na klasikal na pag-encrypt ay hindi pa umiiral, ang retrospective decryption ay isang tunay na banta
- Ang impormasyon at mga komunikasyong naka-encrypt gamit ang mga kasalukuyang cryptographic na pamamaraan ay maaaring maharang, at maitago ay ma-idecrypt sa sandaling dumating ang mas makapangyarihang mga kuwantum kompyuter
- Ang kritikal na data na nangangailangan ng pang-matagalang seguridad ay dapat protektahan ngayon



Sertipikadong Pag-encrypt Tunnelled End-to-End

- Ang mga Cellcrypt Federal tunnel ay nagtatapos sa pag-encrypt sa pamamagitan ng mga tunnel na inaprubahan ng NIAP
 - Cellcrypt Federal encryption tunnels sa pamamagitan ng RTP para sa end to end CNSA+QSE voice encryption
 - Ang Cellcrypt Federal protocol negotiated sa pamamagitan ng Session Description Protocol (SDP)
- Ang E2E Encryption ay naghahatid ng matatag na seguridad sa komunikasyon para sa bawat mensahe, tawag, at bidyo call

CNSA Suite Guidelines	Cellcrypt
Advanced Encryption Standard (AES), per FIPS 197, using 256-bit keys to protect up to TOP SECRET.	AES-256 Fully Compliant
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange, per FIPS SP 800-56A, using Curve P-384 to protect up to TOP SECRET.	Fully Compliant (also supports P-521)
Elliptic Curve Digital Signature Algorithm (ECDSA), per FIPS 186-4, using ECDSA-384 to protect up to TOP SECRET.	Fully compliant (also supports P-521)
Secure Hash Algorithm (SHA), per FIPS 180-4, using SHA-384 to protect up to TOP SECRET.	Fully compliant (also supports SHA-512)



Sertipikadong Pag-encrypt

Isang Multi-Layer na Cryptographic na Diskarte

1. Na-obfuscated ang data
2. Naka-encrypt gamit ang CNSA Cryptography
3. Sa Post-Quantum Protection
4. Tumatakbo sa pamamagitan ng isang NIAP Architecture

Cellcrypt Federal

Authenticated, end to end na naka-encrypt na pagmemensahe, boses, video

- Ang pagmemensahe, pagtawag/bidyo, at malalaking paglilipat ng file ay ganap na naka-encrypt dulo sa dulo (E2EE)
- Inaalis ng Mutual Authentication para sa lahat ng partido ang mga panganib sa spoofing at eavesdropping (MiTM).
- Mga ligtas na grupo para sa pagmemensahe, pagtawag, at pagbabahagi ng file
- Agnostic ang device (iOS, Android, Windows) na may pinahusay na Proteksyon ng "Data at Rest".
- Mga advanced na code para sa kalidad ng HD at low bandwidth mode para sa anumang network, hal., 5G, 4G/LTE, 3G/HSDPA, 2G/EDGE, Wi-Fi, satellite
- Interoperability sa 3rd Party NIAP device at PBX desk phone



Cryptographically Palibutan ang End-User

- Binibigyang-daan ng Cellcrypt na paghiwalayin ang mga komunikasyon at magpatakbo ng maraming branded na app nang sabay-sabay
- Para sa Pamahalaan, maaari nitong paghiwalayin ang mga komunikasyon sa pagitan ng Classified at Unclassified
 - Cellcrypt Federal (Orange App) – On-Premises o Tactically Deployed Classified (Red) Network
 - Cellcrypt (Blue App) – Cloud na naka-host na Unclassified; Mga Kaibigan at Pamilya; Pagtawag sa kapakanan
- Ang parehong mga app ay NIAP/CSfC at nagbibigay ng parehong antas ng sertipikadong pag-encrypt
- Nag-aalok ng parallel redundant network na may parehong katiyakan ng mga komunikasyon





Cellcrypt Federal

- Nag-aalok ang Cellcrypt Federal ng isang maaasahan at secure na solusyon sa komunikasyon na nakakatugon sa mga pangangailangan ng Gobyernong antas na seguridad hanggang sa Classified Secret at Top Secret Communications
- Buong katiyakan para sa mga komunikasyon kahit sa pinakamahirap na kapaligiran habang nag-aalok ng natatanging cryptographic na diskarte na nag-aalis ng pangangailangang magtiwala at umasa sa seguridad ng Walled Garden



Cellcrypt[®] FEDERAL



WALANG PAGTITIWALA
MGA LIGTAS NA KOMUNIKASYON
& DATA-IN-TRANSIT

