Cellcrypt® FEDERAL

ZERO-TRUST
SECURE COMMUNICATIONS
& DATA-IN-TRANSIT

CSfC

FIPS VALIDATED 140-2

Cellcrypt FEDERAL

Trust in a Zero-Trust World

- Full assurance for communications and data-in-transit even in austere, proactively compromised ‘Zero-Trust’ environments

Cellcrypt FEDERAL

Cellcrypt Federal

- Full assurance for communications and data-in-transit even in austere, proactively compromised ‘Zero-Trust’ environments

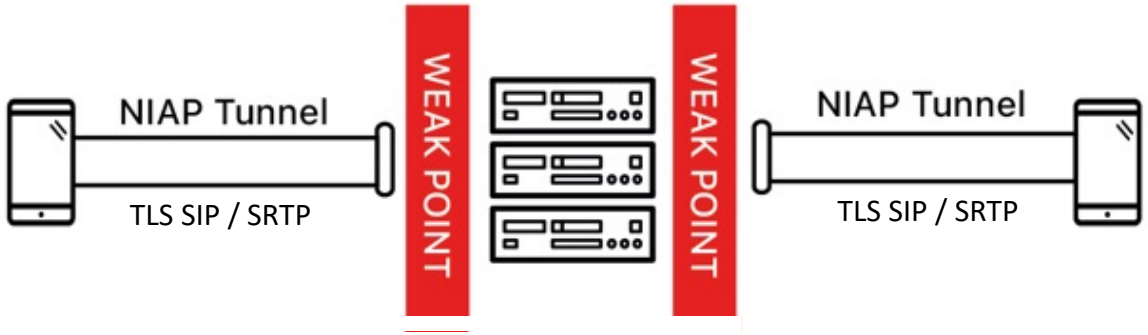
Cellcrypt FEDERAL

Cellcrypt Features

Authenticated, E2E Encrypted Messaging, Voice, Video

- Messaging, voice/video, and large file transfers are fully-encrypted end-to-end (E2EE).
- Mutual Authentication for all parties eliminates spoofing and eavesdropping (MiTM) risks
- Secure groups for messaging, calling, and file sharing
- Device (iOS, Android, Windows) agnostic with enhanced “Data at Rest” Protection
- Advanced codecs for HD quality and low bandwidth mode for any network, e.g., 5G, 4G/LTE, 3G/HSDPA, 2G/EDGE, Wi-Fi, satellite
- Interoperability with 3rd Party NIAP devices and PBX desk phones

Walled Garden



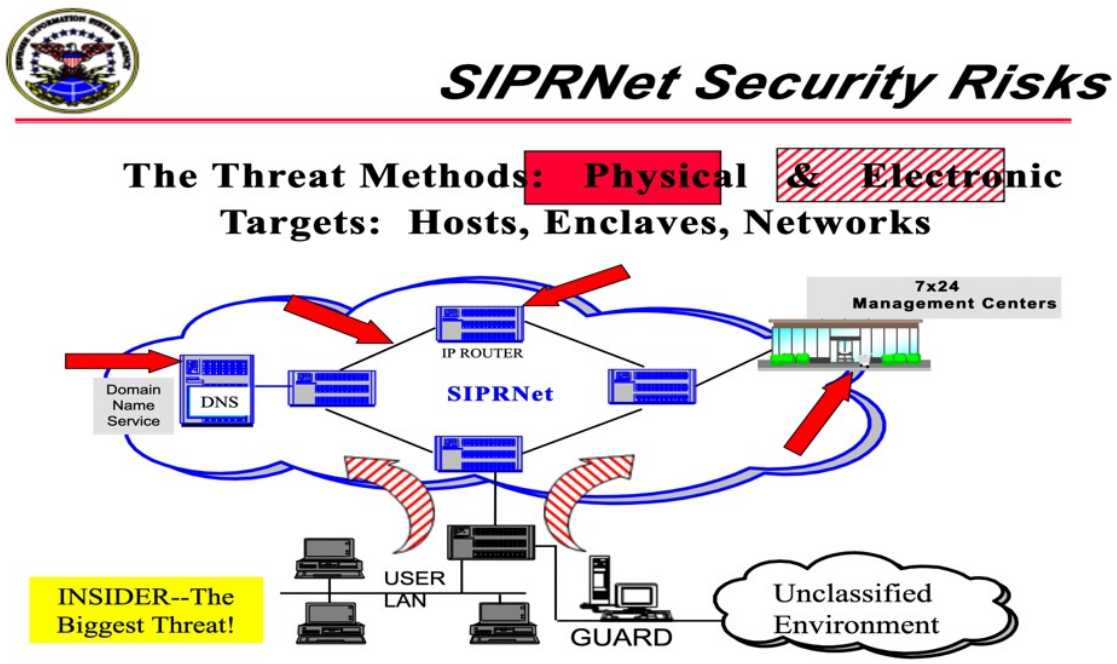
Cellcrypt FEDERAL

The Walled Garden
A "Trusted" Network

- Many solutions rely on 'trust' in a "Walled Garden" i.e., companies that provide the solution, individuals that run the system and security of the network

Walled Garden

Cellcrypt FEDERAL



The Walled Garden
A "Trusted" Network

- Walled Gardens are vulnerable to a number of threats and do not tackle the greatest problem – the INSIDER – the biggest threat as acknowledged by DISA

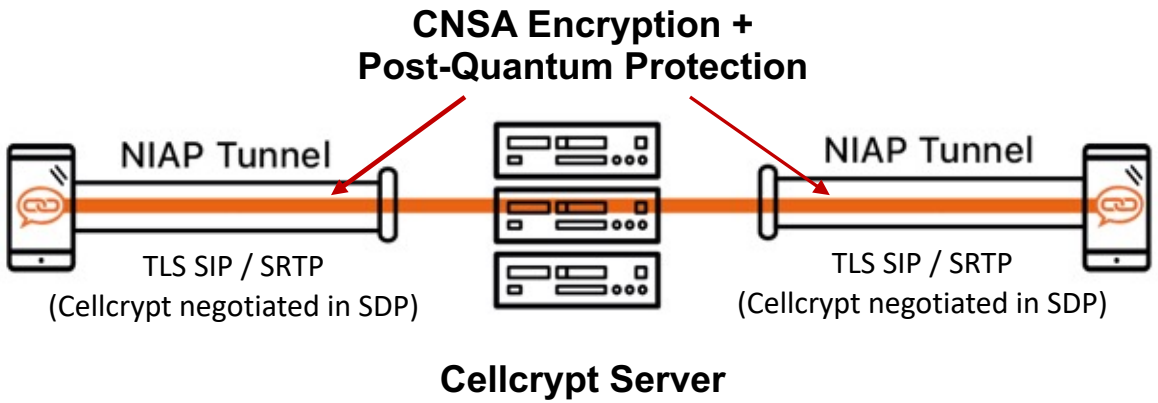
Cellcrypt FEDERAL

Harvest Now, Decrypt Later

The Quantum Computing Threat

- Although quantum computers powerful enough to break the strongest classical encryption do not exist yet, retrospective decryption is a real threat
- Information and communications encrypted with current cryptographic techniques can be intercepted, stored and later decrypted once more powerful quantum computers arrive
- Critical data requiring long-term security should be protected now

Walled Garden



Cellcrypt FEDERAL

Tunneling End-to-End Encryption
Solves the Problem

- Cellcrypt Federal tunnels end-to-end encryption through NIAP-approved tunnels
  - Cellcrypt Federal encryption tunnels through RTP for end-to-end CNSA+QSE voice encryption
  - Cellcrypt Federal protocol negotiated via Session Description Protocol (SDP)
- E2E Encryption delivers robust communication security for every message, voice, and video 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)

Using the NIST P-521 curve, the largest key size specified, gives an overall key strength equivalence of 256 bits.

Cellcrypt FEDERAL

Cellcrypt Encryption

Multi-Layer Cryptographic Approach

1. Data is Obfuscated

All data - voice, video, messages, and file attachments - are first obfuscated using the ChaCha20-256 algorithm to mitigate any future potential AES vulnerabilities. This occurs before the data is encrypted through the Cellcrypt Crypto Core.

2. Encrypted with CNSA Cryptography

The obfuscated data is secured end-to-end using a package of Elliptic Curve Cryptography (ECC) and Symmetric-Key Cryptography that meets or exceeds the key length standards of the CNSA Suite for Top Secret communications.

Cellcrypt FEDERAL

Cellcrypt Encryption

Multi-Layer Cryptographic Approach

3. With Post-Quantum Protection

Cellcrypt's Crypto Core is then cryptographically overlaid with Post-Quantum Cryptography. The quantum-safe envelope allows for algorithms (such as CRYSTAL-KYBER and Classic McElise) to be layered and changed as standards in this area emerge without affecting the strength of the underlying ‘classical’ CNSA encryption.

4. Running through a NIAP Architecture

All data and cryptography detailed is run through a NIAP validated MA CP 2.5 compliant architecture where the outermost layer and all server links are secured with TLS using NIST validated algorithms (ECC-384 and AES-256).

Cryptographically Surround the End-User

- Cellcrypt allows you to segregate communications and run multiple branded apps simultaneously
- For Government, this can segregate communications between Classified and Unclassified
  - Cellcrypt Federal (Orange App) – On-Premises or Tactically Deployed Classified (Red) Network
  - Cellcrypt (Blue App) – Cloud hosted Unclassified; Friends & Family; Welfare calling
- Both apps are NIAP/CSfC and provide the same level of certified encryption
- Offers a parallel redundant network with the same assurance of communications

What is the Value to Government and Military?

- Cellcrypt Federal offers a reliable and secure communication solution that meets the needs of government for protecting `Unclassified to Classified comms against the evolving threat landscape
- Cellcrypt Federal provides full assurance for communications in even the toughest environments while offering a unique cryptographic approach that eliminates the need to trust and rely on the security of the Walled Garden

Cellcrypt® FEDERAL

ZERO-TRUST
SECURE COMMUNICATIONS
& DATA-IN-TRANSIT

CSfC

FIPS VALIDATED 140-2