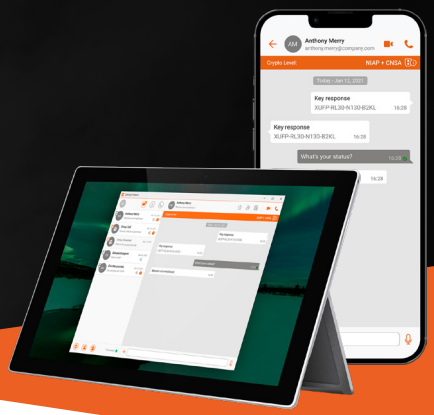
Cellcrypt FEDERAL

EXCEEDING THE STANDARD FOR US TOP SECRET COMMUNICATIONS



The Challenge:
Trust in a Zero-Trust Environment

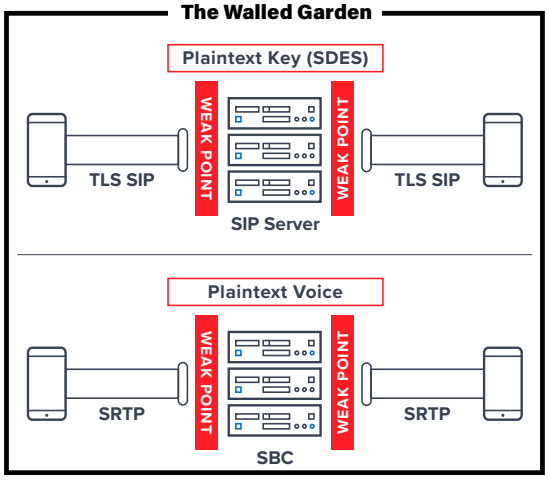
Despite their advocacy for Zero-Trust Environments, governments around the world are relying on fully trusted "Walled Garden" environments to protect even their most highly classified information.

The practical implications of this include:

- Need for VPN/Dual-VPNs for internet-based users
- Restrictions on the type of device approved for use within those environments
- Quality of Service issues (e.g., dropped/slow VPNs, roaming problems, etc.)

In addition, many soltutions rely on the use of point-to-point TLS/SRTP links alone to protect communications, however this can introduce weakness/point of intercept at the server. The current approach to resolving this issue is to put the server into the trusted zone, i.e., the "Walled Garden".

There we find the contradiction in trusting the network while advocating a Zero-Trust approach.



The Solution:
End-to-End Encryption with Post-Quantum Protection through the Tunnel

Cellcrypt Federal encryption tunnels Commercial National Security Algorithm Suite (CNSA) cryptography with Post Quantum Cryptography (PQC) through TLS SIP and SRTP channels to provide end-to-end message/voice/video encryption.

Cellcrypt Federal:
A Multi-Layer Approach to Cryptography that Exceeds the Standards for US Secret & Top Secret

1. NIAP Validated to protect US Govt. Classified Data

Cellcrypt is NIAP validated to operate in an MA CP 2.5 architecture. The outermost layer and all server links are secured with TLS using NIST validated algorithms (ECC-384 and AES-256).

This architecture is validated to protect US Classified Secret and Top Secret communications. Cellcrypt Federal provides this as a baseline but adds E2E encryption tunneled through the architecture.

2. Obfuscation

All data - voice, video, messages, and file attachments - are 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.

3. Commercial National Security Algorithms (CNSA)

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

CNSA Suite Comparison	Cellcrypt Crypto Core
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.	ECDH-521 **Exceeds Guideline**
Elliptic Curve Digital Signature Algorithm (ECDSA), per FIPS 186-4, using ECDSA-384 to protect up to TOP SECRET.	ECDSA-521 **Exceeds Guideline**
Secure Hash Algorithm (SHA), per FIPS 180-4, using SHA-384 to protect up to TOP SECRET.	SHA-512 **Exceeds Guideline**

Using AES-256 together with ECC-521 (NIST P521) provides an overall 256-bit key strength.

4. Post-Quantum Cryptography (PQC)

Cellcrypt's Crypto Core is then cryptographically overlaid using Supersingular Isogeny Diffie-Hellman Key Exchange (SIDH 751) for Voice and Supersingular Isogeny Key Encapsulation (SIKE 751) for Messaging and Files.

Secure Communications for Government

www.cellcrypt.com

CELLCRYPT FEDERAL FEATURES

Authenticated, E2E Encrypted Messaging, Voice, Video

- Messaging, Voice, Video fully encrypted End-to-End
- Secure Groups for Messaging and Voice (Video in Q2 ’22)
- Mutual Authentication for all communications, including groups (removes spoofing risk)
- Device Agnostic (iOS/Apple Mac (M1+), Android, Windows)
- Network Agnostic: 5G, 4G/LTE, 3G/HSDPA, 2G/EDGE, WiFi, satellite networks
- Advanced Codecs for HD quality Voice/Video
- Low Bandwidth Mode for austere environments
- Interoperability with 3rd-Party NIAP validated devices and PBX desk phones
- Kill Code and Remote Wipe capabilities

Cryptographically Surround ALL Your Users

- Segregate communications by running two Cellcrypt Stacks and apps simultaneously, for instance:
  - Cellcrypt Client #1 on Stack #1:
    - Official Use (Unclassified/CUI to Top Secret)
  - Cellcrypt Client #2 on Stack #2:
    - Coalition Partners
    - Welfare/Personal
- Both apps provide the same strength encryption.
- Running two Stacks offers redundant parallel networks.
- Provision App via MDM (e.g., MobileIron) or Consumer App Stores
- LDAP/Active Directory integration
- Datacenter, private cloud and multi-cloud deployment options provides control over users, devices, policies and metadata.

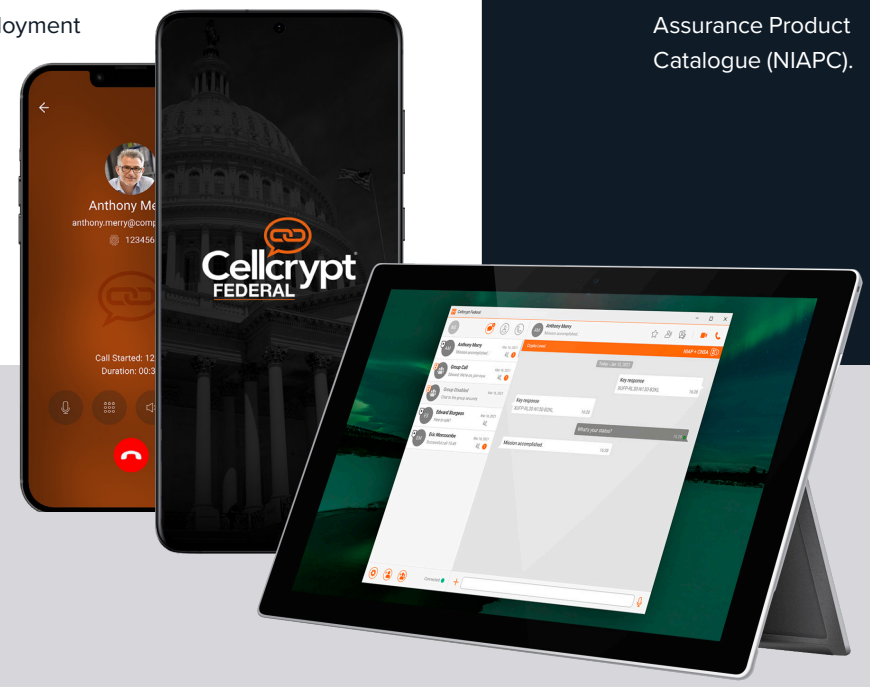
Cellcrypt Validations and Certifications

Cellcrypt is validated by the US National Information Assurance Partnership (NIAP) under its Common Criteria Evaluation and Validation Scheme (CCEVS).

Cellcrypt is certified by the National Institute of Standards and Technology (NIST) to FIPS 140-2.

Cellcrypt products have been validated for use as a Voice over Internet Protocol (VoIP) component in a Commercial Solutions for Classified Solution (CSfC).

Cellcrypt’s Secure Voice Over IP products are on the NATO Information Assurance Product Catalogue (NIAPC).



Cellcrypt
TRUSTED COMMUNICATIONS

Download Cellcrypt today:

www.cellcryptfederal.com