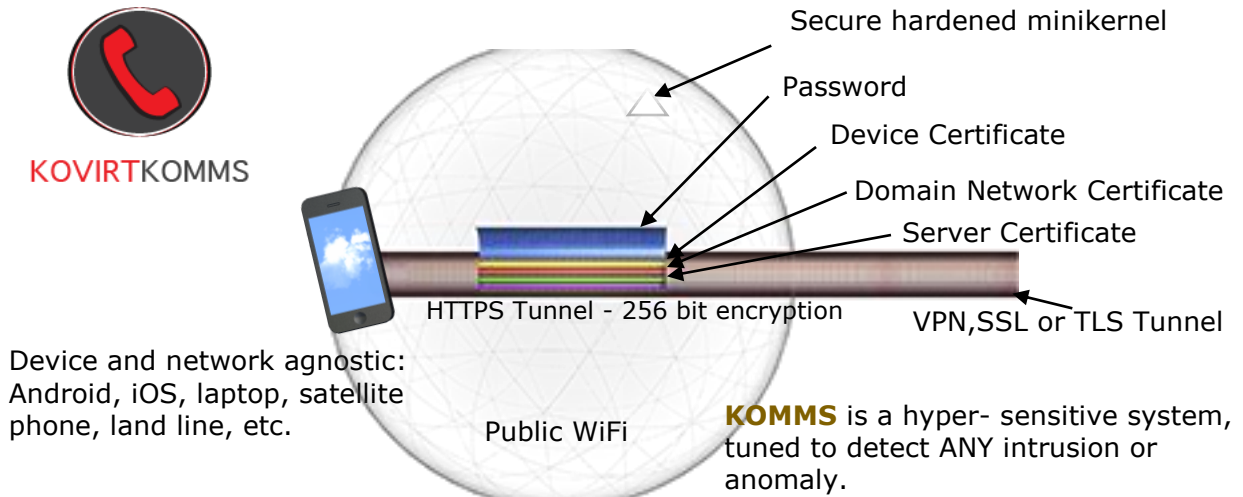# Quiet, please.

Do you have projects that require private communications among team members? Are you concerned that data compromise can occur with unsecured hardware and software across your enterprise? Do you need to limit communication of information to certain groups at certain times? Does the threat of exposure for your most sensitive data keep you up at night? If you answered "yes" to any of the above questions, ICE ITS would like to introduce you to **SCCS**, our secure cloud communication services.

Let's just keep this between us.

Think of **SCCS** as an exclusive community - a closed sphere of influence in which your data (voice, text, video, etc.) can move freely without fear of compromise. We provide tailored solutions that allow you to determine the level of protection: who's in and who's out and what type of services you need. Communicate person-to-person, group-to-group or group to person. Our flexible infrastructure and software architecture allow for a wide variety of configurations - use *any device* across *any network*.

KOVIRTKOMMS

Secure hardened minikernel

Password

Device Certificate

Domain Network Certificate

Server Certificate

HTTPS Tunnel - 256 bit encryption

VPN,SSL or TLS Tunnel

Device and network agnostic:
Android, iOS, laptop, satellite phone, land line, etc.

Public WiFi

KOMMS is a hyper- sensitive system, tuned to detect ANY intrusion or anomaly.

Do you want to hear a secret?

Our methods employ the world's most stringent encryption and authentication strategies to ensure the highest grade of security and obfuscation.

- **Global**: Worldwide private backhaul with virtual endpoints in over 134 countries.
- **Maximized**: High efficiency routing for optimum throughput.
- **Integrated**: Each endpoint issued is integrated but private - including video, phone, text, chat, drop-box, email, and secure FTP.
- **Virtualized**: All aspects can be instantly launched, dissolved, relocated and/or archived.
- **Flexible**: Device and network agnostic - no specialized hardware. Plus, each instantiation can run independently or as part of a global enterprise.
- **Scalable**: Due to the unique architecture, new endpoints can be established quickly in rapid or expeditionary scenarios as necessary.
- **Secure**: Next generation polymorphic encryption including 7-factor authentication.