



## Encrypted Telephony Breakdown

### Hardware

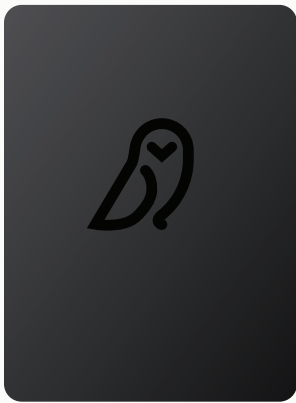
- Dispel Wicket (On-site access for phones/desktops)

### Access Layer

- Dispel Enclave (End-to-End Encryption)

### Protected Internal Resources

- Telephone Server (extension dialing & conferencing)



Hardware

### Dispel Wicket

Connects any Internet enabled device (or group of devices) to a specific Enclave.



## Encrypted Telephony

### Encrypted communications for an Energy Utility Provider

In 2018, Dispel started working with an energy utility provider to enable facility-to-facility and facility-to-board telephony and teleconferencing across nuclear power plants. These communications must exist entirely off channel — meaning without exposure to public surveillance or compromise — and must be available on desk phones, as well as desktop and mobile devices.

Dispel provided the energy company with a PBX phone server deployed within a Dispel Enclave. Onsite at the power facilities, Dispel Wickets ensure encrypted connections to the Enclave. Board members and other privileged offsite users access the Enclave through the Dispel application on their desktop and mobile devices.

Within the Enclave, the phone server provides full internal extension dialing, conference calling, call recording, and voicemail.