Quantum Bridge

Product Data Sheet

Black Phone

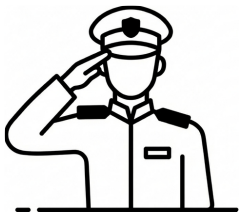
Quantum-safe, end-to-end encrypted mobile communication solution protected by DSKE

Security by Design, Control by Default

Organizations operating in sensitive environments cannot afford to trust third-party infrastructure with their most critical communications. Black Phone gives organizations complete ownership of their secure communications — a mobile messaging and voice platform where data and encryption keys never leave your infrastructure, and no external party can ever access your conversations.

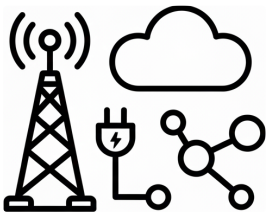
Available on iOS and Android, Black Phone enables quantum-safe messaging, voice calls, and file exchange across your organization. It is deployed entirely within your own environment — on-premises or in your private cloud — meaning your data, your keys, and your communications remain under your exclusive control.

Industries



Government & Defence

Financial Institutions



Telecom & Critical Infrastructure

What is DSKE?

Distributed Symmetric Key Establishment (DSKE) is a key establishment protocol uniquely based on symmetric cryptography. Multiple Security Hubs independently distribute cryptographic material (PSRD) to clients. Clients can then use the Security Hubs as brokers to negotiate symmetric keys which can be used to authenticate and encrypt further communication. As Security Hubs are independent of each other, the final DSKE keys are only known to the clients, leveraging a secret-sharing scheme, which also provides reliability against Hub failure or compromise.

Key Features

- Future-proof End-to-End encryption
- Chat and voice calls support
- Symmetric key security with DSKE
- Data sovereignty
- Easy onboarding process
- On-prem or cloud solution
- Group collaboration features

Security

- Key exchange: DSKE and X25519 exchanges in parallel, two 256-bit keys mixed with XOR
- AES-GCM symmetric encryption for messages, files and calls based on previously exchanged keys
- Hardware-protected key storage
- OS-provided file encryption for locally-stored data
- TLS for all communication
- Back-end database row-level security based on user authentication

Management

- Centralized user provisioning and deprovisioning
- Monitoring dashboard
- Policy management for rotation of cryptographic material
- Compliance reporting and audit logs
- Role-based access controls

Contact Us

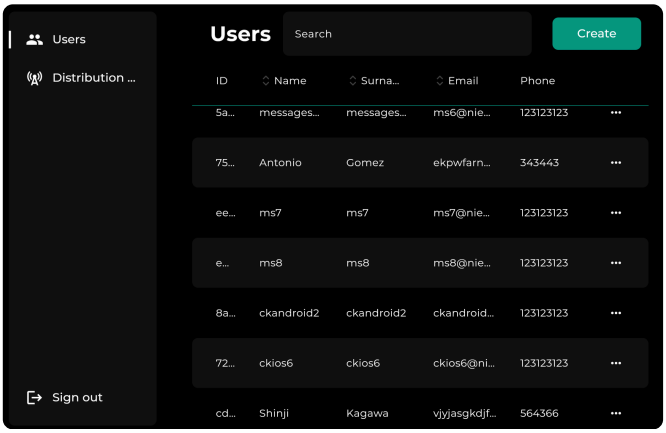
+1-249-225-5099

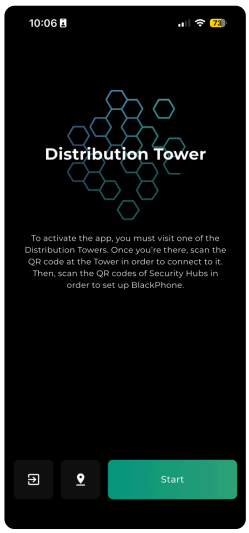
contact@qubridge.io

Deployment

Install Black Phone Admin

Black Phone Admin is deployed on-premises to streamline user creation and onboarding. It integrates with Security Hubs to authorize new PSRD generation, ensuring secure delivery to users during setup.



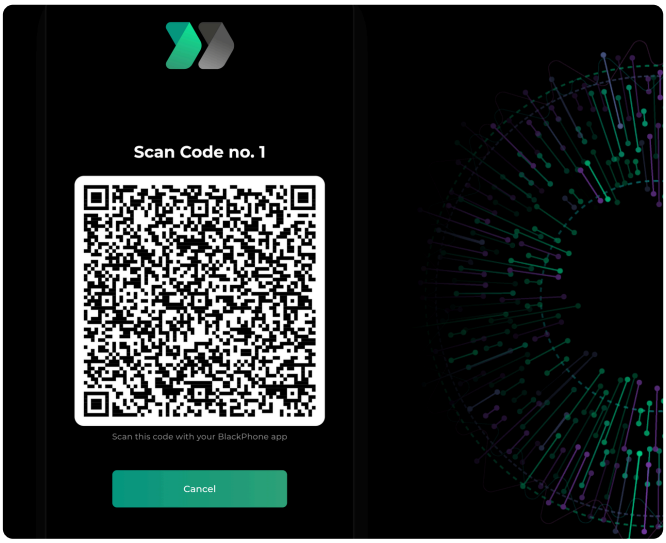


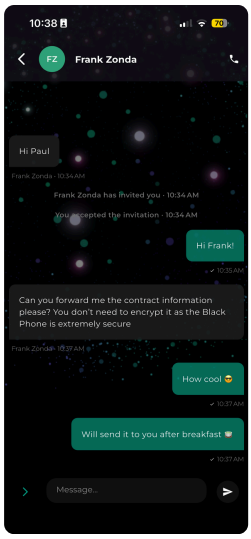
Download Black Phone App

Users download and install the Black Phone app on their devices, supplying only the minimal information needed for identification by the manager and guided to the nearest Distribution Tower.

Deliver Activation Tokens

To activate a Black Phone, users receive a unique QR code from each Security Hub. These codes can be distributed through corporate mail or delivered automatically via PSRD Distributor Towers on site.





Communicate and Monitor

Once activated, users can communicate securely, with cryptographic keys updated automatically as needed. Managers may periodically require users to re-authenticate with updated tokens, based on organizational policies.