Your Data in Your Control

Enabling Secure, Controlled, and Private Data Sharing

Prepared for
Privitty Engineering
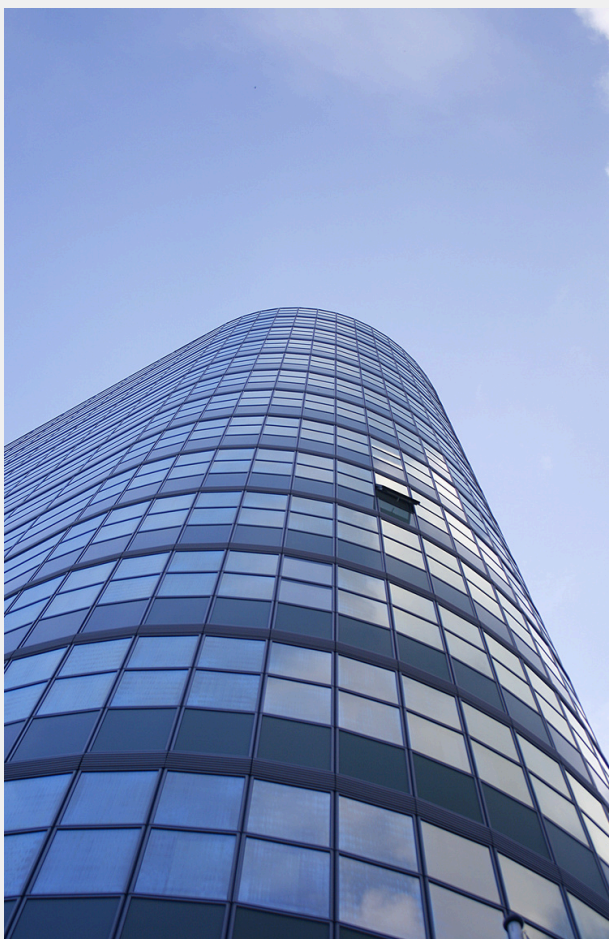
Presented to
Partners

Presented by
Milind Deore

Agenda

Privitty: Redefining Data Ownership and Security in a Zero-Trust World

A platform-agnostic solution for end-to-end encrypted, policy-driven data sharing.

In today's digital economy, data is the most valuable asset — yet it's constantly at risk.

Privitty empowers businesses to share information securely, with **end-to-end encryption, portable access controls, and zero-trust design**.

Whether across messaging platforms, collaboration tools, or cloud storage, Privitty ensures **your data stays yours — always**.

Powered by advanced cryptography and proven communication protocols like **Delta Chat**, Privitty delivers uncompromising privacy in motion.

Who We Are?

2024	Your firm is founded
6	Employees
1	Office in Bangalore, India
2	Founders with successful Exits

Founded in 2024 by a team of seasoned technologists, Privitty brings together over 20 years of expertise in semiconductors, embedded systems, AI, and cybersecurity.

With a portfolio of granted patents and prior successful exits, we're building Privitty with a singular mission:

To give businesses complete control over their data — wherever it goes.

Our Mission

Privitty builds a door only you control—not just more locks.

Our Mission:

To empower organizations with uncompromised data security, privacy, and control — no matter where the data travels or resides.

Unlike AI-based threat detection tools that rely on probability, **Privitty uses cryptography, not guesswork**. Our approach ensures protection **100% of the time** — deterministic, tamper-proof, and enforceable.

Problem: Trusting the Pipe Instead of Protecting the Payload

70%
Breach Due
To Insiders

25%
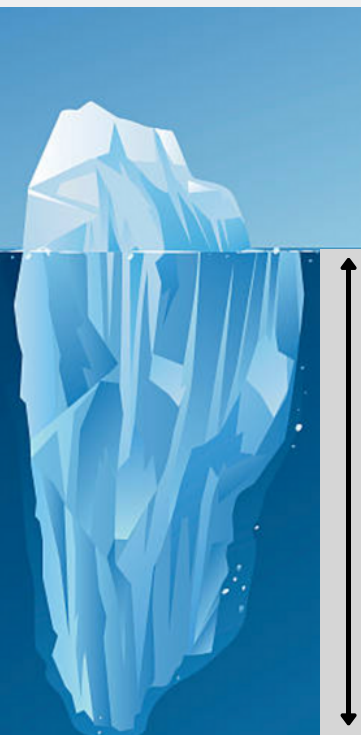Slip-Ups, Wrong
Peers

$M
1 Mistake = Millions Lost +
Reputation Destoryed

Insider Threats Are Killing Enterprises

Access to
Sensitive Data

Human Errors

Slip-Ups

Wrong Peer

Intentional

Traditional messaging and file-sharing platforms are built for convenience — not control. They are:

- Centralized, with limited encryption,
- Prone to insider threats and human error,
- Over-reliant on server-side enforcement.

The result? One accidental forward or bad actor can cost millions — and reputation.

What's needed is a data-centric protection model:

- That travels with the data
- Enforces control even when forwarded
- Works across devices and platforms
- Operates without trusting the network or app

This is exactly what Privitty delivers.

The Privitty Approach

Core Principles

- 🔐 End-to-End Encryption: All content is encrypted on the sender's device and decrypted only by intended recipients.

- 📇 Portable Access Control: Policies travel with the data — even across platforms or apps.

- 🚫 Zero-Trust Architecture: No assumption of trust in networks, servers, or apps.ero Trust by Design – Privitty assumes untrusted networks, apps, and servers.

- 🌍 Platform Agnostic: Works across messengers, file-sharing tools, cloud apps, and APIs.

Key Features & Capabilities

At Privitty, we believe enterprises deserve better—proactive protection, not reactive regrets. Because in a world where trust is your most valuable currency, you can't afford to lose it.

Welcome to **Privitty**

Privitty is a secure, decentralized messaging app with advanced privacy features like message revocation and time-limited access.

- True Revoke,

- Allow peer to download, forward,

- Time based access,

- Know who has your data,

- Complete message tracing,

- Device native with out intermediary,

- Modern cryptographic primitives, forward & backward secrecy, post-compromise security.

- Mobile and Desktop SDK,

- Support most of the documents, image, video formats.

- Multiple patented idea to manage keys.

How It Works:
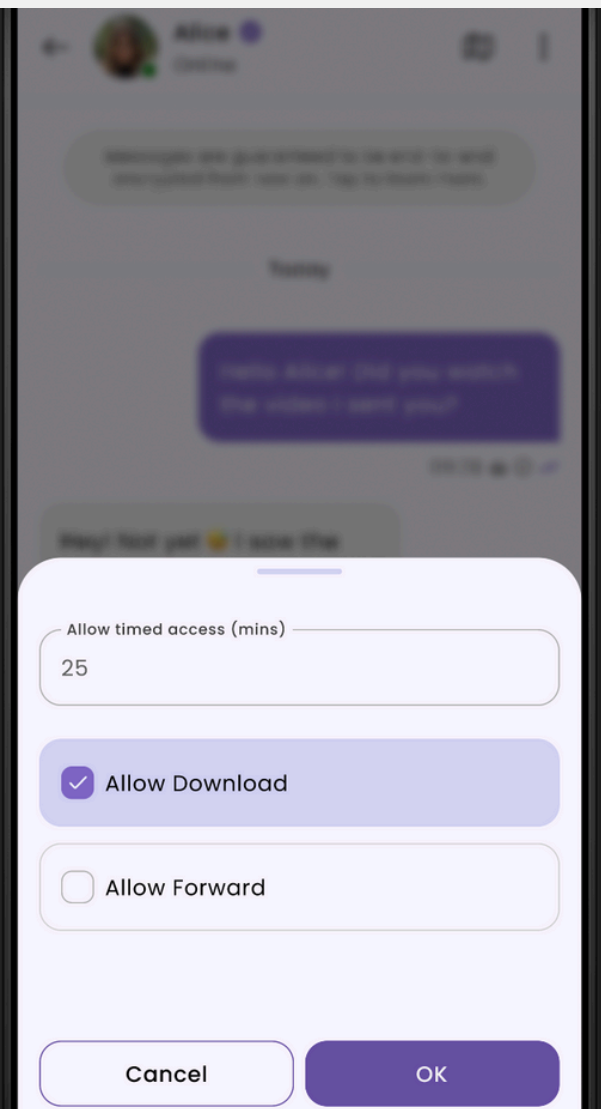
01 File & Message Encryption

The sender encrypts files or messages using a hybrid encryption model:

- Symmetric encryption (AES-GCM) for content.
- Asymmetric encryption (X25519 or RSA) to share keys securely with recipients.

02 Access Control Metadata

Every encrypted item includes:

- A policy blob (who can open, expiry, re-share restrictions),
- Cryptographic signatures and hashes to validate content integrity.

03 Privitty Envelope Format

Packaged into a custom .priv format (or embedded JSON blob for messages).

Contains:

- Encrypted content,
- Metadata,
- Versioning,
- Forwarding restrictions,
- Optional audit log.

How It Works ...

04 Secure Client Libraries

These libraries are built to integrate seamlessly across platforms and are tested over robust messaging backbones such as the open-source Delta Chat platform — ensuring reliability at scale while maintaining full user-side control.

Responsible for:
- Encryption/decryption,
- Signature verification,
- Message/event handling.

Case Studies
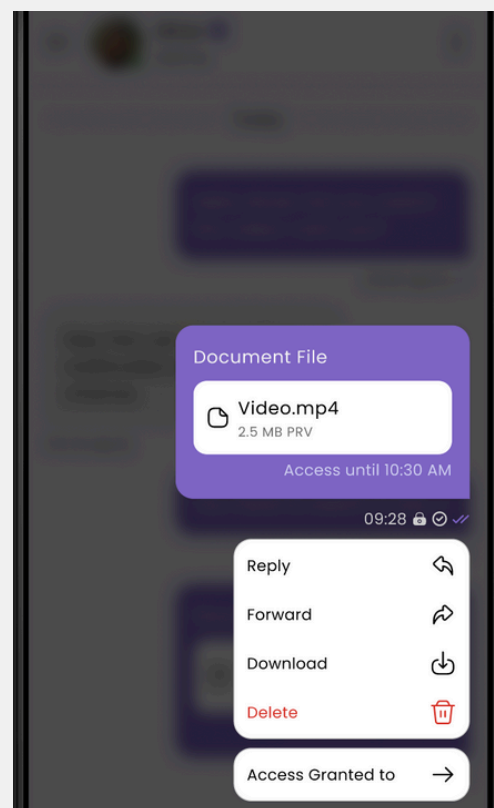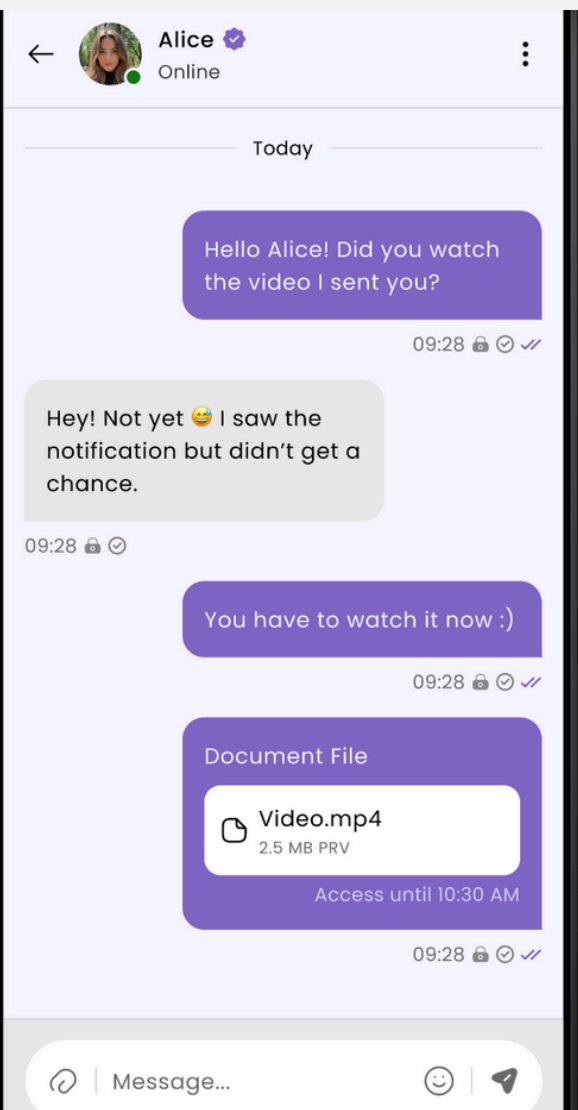
- Secure file sharing in enterprise and legal settings.
- Health records transmission with per-recipient access.
- Zero-trust collaboration between organizations.
- Whitelabel messengers with E2EE & custom access control features.

Estimated Gains

80 - 95%

Finance - Risk reduction

---

70 - 90%

Legal - Audit trail clarity

100%

Regulatory compliance

---

60 - 85%

IP leak prevention

Timeline

Whether you're building secure communication tools, handling sensitive files, or simply want to guarantee privacy by design — Privitty is ready.

01 Android - LIVE

GET IT ON
Google Play
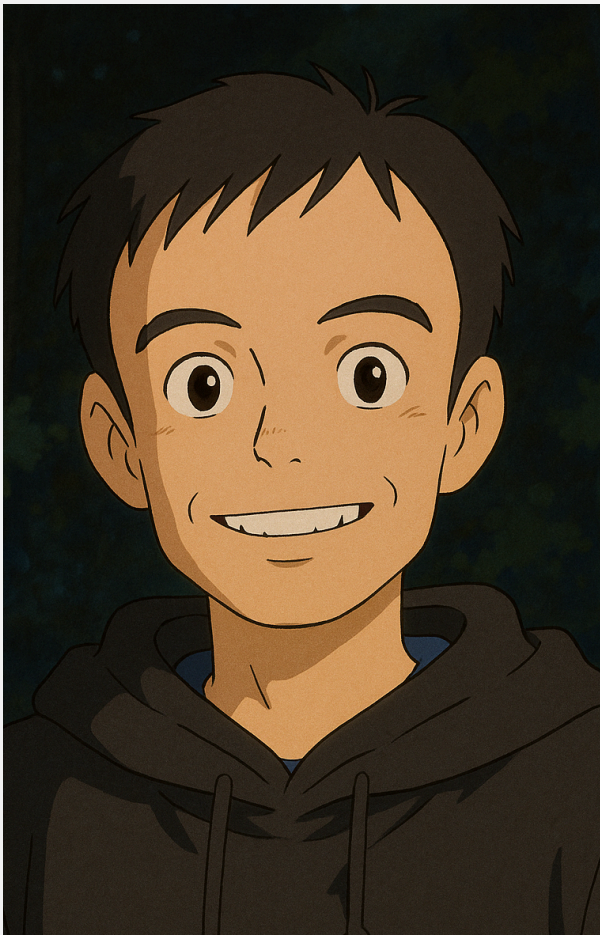
02 iOS

Launching in a month i.e. August, 2025

03 Desktop

Launching on macOS, Windows, Linux in a month i.e. August, 2025

Ready to Take Control of Your Data?

Milind Deore

📞 +91 - 91759 64875

✉ mailus@privittytech.com

🌐 www.privittytech.com

Thanks

Privitty builds on the proven transport and encryption layers of Delta Chat, an open-source E2EE messenger based on the Autocrypt standard.