# SurePack: Anonymous, Quantum-Resilient Secure File Sharing

## The Problem: Insecure File Sharing is Costly and Outdated

Despite living in an age of daily cyber threats and strict data regulations, businesses still struggle with secure file transfer. **Employees routinely bypass IT safeguards** – *71% of office workers globally admit to sharing sensitive company data through unauthorized messaging and collaboration tools*. This behavior exposes organizations to breaches and compliance penalties. In Australia, the **average data breach now costs AUD $4.26 million** (≈USD $2.8M), a **27% increase** since 2020. Such incidents aren't rare – phishing and stolen credentials are leading causes – and they underscore a critical need for better secure communication channels.

Meanwhile, traditional encryption solutions have failed to gain broad adoption due to complexity. **PGP, once the go-to tool for encrypting files/email, is now considered antiquated** – security experts bluntly state that "PGP is bad and needs to go away". Its 1990s design and clunky user experience mean that **no competent crypto engineer would build a system like PGP today**. Usability studies famously showed even tech-savvy users struggling for hours to set up PGP properly. In practice, most people simply won't use such cumbersome tools, leaving sensitive files unencrypted and sent over email or consumer cloud drives. The bottom line: **organizations lack a user-friendly, modern way to share files with strong end-to-end encryption**. This gap between security needs and practical tools presents a major opportunity.

## The Solution: SurePack Overview

**SurePack** is a next-generation secure file transfer platform designed to fill that gap. It delivers **end-to-end encrypted file sharing with anonymity and ease of use** – essentially *"PGP for 2025"* but without the pain points. SurePack consists of two main components:

- **Suredrop (Server):** A lightweight ASP.NET Core REST API server that acts as a secure relay and public-key directory. It stores users' public certificates and encrypted files (packages) in the cloud (using AWS S3), but **never has access to any unencrypted data**.
- **SurePack (Client):** A cross-platform client (CLI and GUI) that lets users create, send, and receive encrypted packages. The client handles all cryptography locally – keys are generated and managed on the user's device, ensuring **private keys never leave the client**.

**How it works:** Users generate an **anonymous digital identity** (an X.509 certificate) with a simple command. The system produces a random, memorable alias comprising three words (e.g. `crow-mandate-current.publickeyserver.org`) as the certificate name. This serves as the user's public address on the Suredrop server. **No personal details or login are required** – the design follows an *Anonymous Certificate Enrollment (ACE)* protocol, meaning anyone can obtain a certificate without disclosing their real identity. (If desired, an email or name can be optionally bound to the cert, but it's not required.) The three-word alias is easy to communicate and verify, unlike long PGP key fingerprints. It's even a valid DNS name – entering the alias URL in a browser will fetch that user's public key certificate for verification.

With an alias in hand, secure sharing becomes straightforward:

- **Packing & Encryption:** A user can select files (say, `contracts/*.pdf`), choose one or more recipient aliases, and "pack" them into a **SurePack** encrypted package. Under the hood, each file is compressed and split into chunks, then encrypted with a fresh 256-bit AES key in GCM mode. For each recipient, that AES key is encrypted with the recipient's RSA-2048 public key, and then that RSA key cipher is *again encrypted using a Kyber1024 post-quantum key encapsulation*. This hybrid encryption (`AES-GCM + RSA + Kyber`) ensures both **classical security and quantum resilience**. Even if RSA-2048 is cracked in the future, the additional Kyber layer means the file's AES key remains safe. Cryptography is implemented with proven libraries (Bouncy Castle), and all steps are **fully automated** for the user.
- **Sending:** The client then signs the package (for authenticity) and sends it to the Suredrop server via a simple `POST /package/{recipient}` API call. The server, knowing each recipient's public key, **stores the encrypted package in that recipient's "dropbox"** on S3. The server cannot read the contents – it only sees envelope metadata and the opaque encrypted blobs.
- **Receiving:** A recipient can list and download incoming packages addressed to their alias (via `surepack list` and `surepack receive` commands or GUI clicks). Upon receiving, the SurePack client will use the recipient's private key to decrypt the small AES key (layered via Kyber+RSA) and then decrypt all file contents. The result is the original files, intact and secure. Because each package used a one-time AES key, **Perfect Forward Secrecy** is achieved – compromising one package's key reveals nothing about others.

From a workflow perspective, **SurePack feels simple: users exchange human-readable aliases, not long keys; creating and sending an encrypted bundle is as easy as zipping files; and receiving is as easy as checking an inbox.** All the complexity (key generation, encryption, signature, server upload/download) is handled behind the scenes by the SurePack client and server.

## Key Features and Innovations

**1. Anonymous PKI with Easy Verification:** SurePack introduces an **Anonymous Certificate System** that provides the trust of Public Key Infrastructure (PKI) without the usual overhead. The three-word random aliases act like self-chosen email addresses for encryption. This design offers **several advantages**:

- **No Identity Needed:** Users can get a certificate alias instantly, without paperwork or a Web-of-Trust ceremony. This lowers the barrier to adoption – anyone can start encrypting within minutes.
- **Memorable Aliases:** The random phrase alias (e.g. `crow-mandate-current`) is easy to read and communicate compared to a 40-character PGP key hash. It's unique (collision chance is astronomically low) and tied to our server's domain for authenticity.
- **Built-in Verification:** Because each alias corresponds to a live URL on the server (e.g. `https://crow-mandate-current.publickeyserver.org`), **verifying someone's public key is as simple as visiting their alias URL**. The server will present their certificate (which browsers can check against the trusted CA). This provides a user-friendly way to confirm keys, tackling a long-standing PGP challenge of key verification. It's a **simplified validation model** – essentially "if you can reach the alias on our server, you've got the right key," backed by our certificate authority.

*(For cases where identity is important, the system allows optional binding of an email to the certificate and lookup by that identity. But if anonymity is preferred (e.g. whistleblowing, confidential tips, or simply privacy-conscious collaboration), the alias alone suffices.)*

**2. Strong Hybrid Encryption (Post-Quantum Ready):** Each file package is secured through multiple layers, combining time-tested algorithms with cutting-edge cryptography:

- **AES-256-GCM for content encryption:** A robust, industry-standard symmetric cipher provides the actual data confidentiality and integrity (with GCM authentication).
- **RSA-2048 for key encryption:** Widely trusted public-key encryption ensures that only the intended recipient (with their RSA private key) can unwrap the AES key. RSA-2048 has decades of scrutiny and is still deemed secure against classical computers.
- **Kyber1024 for post-quantum security:** SurePack is **ahead of the curve on quantum threats**. Kyber (a lattice-based KEM) was selected by NIST as the primary post-quantum encryption standard. We've integrated Kyber at the top layer, meaning even a future quantum computer cannot break the key exchange. This "belt-and-suspenders" approach (RSA *and* Kyber) future-proofs our encryption – a crucial differentiator as experts warn that quantum computers capable of cracking RSA/DH could be reality **within the next decade**. In fact, the industry has already begun migrating: **13% of TLS 1.3 traffic in 2024 was observed using post-quantum encryption** – early adopters taking the quantum threat seriously. SurePack positions us at the forefront of this shift, offering quantum-resistant security **now**.
- **Digital signatures (SHA-512 with RSA):** Every SurePack package includes a signed manifest and envelope, ensuring that recipients can verify the package indeed came from the claimed sender and hasn't been tampered with. This prevents spoofing or alteration of files. The signatures use SHA-512 hashes with RSA, providing strong integrity checks.

The result is a system that meets or exceeds modern cryptographic best practices. Unlike PGP's dated ciphers and lack of forward secrecy, SurePack employs **forward secrecy by design (one-time keys)** and **up-to-date primitives**. Security engineers have long called for such measures – e.g. key management that is transparent to users, forward secrecy, and **"cryptography that post-dates the Fresh Prince"** (i.e. anything but 1990s algorithms). SurePack delivers exactly these elements in a cohesive package.

**3. End-to-End and Zero Trust:** SurePack ensures that **only the intended recipients can decrypt files** – not even the server operator (us) can read the data. The server simply relays encrypted packages and stores public certs. This aligns with a zero-trust philosophy and gives clients confidence that their sensitive files (financial records, contracts, IP, personal data, etc.) remain private. Even if our server or S3 storage is compromised, the attackers get only gibberish ciphertext. End-to-end encryption is increasingly a baseline expectation – for example, over **90% of web traffic is now sent over HTTPS**, and popular messengers like WhatsApp and Signal have familiarized users with E2E encryption for messages. SurePack brings that same level of protection to file transfers.

**4. Integrated Delivery Network:** Unlike PGP which only handled encryption and left actual delivery to email or other means, SurePack **integrates the delivery mechanism via Suredrop**. The user doesn't have to separately figure out how to share the ciphertext – the system seamlessly provides a drop-box style delivery. This makes it far more convenient to use. It also adds features like **download tracking and expiration** – the server can note when a package was picked up and can enforce one-time download or auto-delete after a period, reducing lingering sensitive data. (Packages are typically removed from the server once all recipients have downloaded, or after a certain time-to-live, to minimize exposure.)

**5. Short-Lived, Revocable Credentials:** Each SurePack certificate (alias) is intentionally **short-lived and disposable** by default. This is a security design choice: if a key is compromised, it limits the damage window. Users are encouraged to generate new aliases over time or for different contexts. (The system could implement revocation lists or automatic expiration to enforce this in future updates.) This contrasts with PGP's

model of long-lived keys tied to identities, which experts criticize as risky. Here, if there's any concern a private key might be exposed, the user can simply create a new alias/certificate and move on – no extensive "web of trust" fallout. **Ephemeral keys and identities** by default make the system more resilient.

**6. Full-Featured Client and API:** The SurePack client already supports a comprehensive set of operations (as a result of our completed development effort). Users can **create identities, pack/unpack files, send/receive packages, list incoming files, verify certificates, and even launch a GUI** for those less command-line inclined. The inclusion of a GUI is important for adoption – many users prefer a simple visual interface, and we have that covered. For power users or integration into other software, the client's CLI and the open RESTful API mean the solution can be scripted or built into other tools. For example, a company could integrate SurePack into an email gateway or a document management system using the API, automatically encrypting outgoing files that meet certain criteria.

In summary, **SurePack's innovation is offering **military-grade security with consumer-grade simplicity**. It eliminates the historical trade-off between security and convenience:

- **No passwords or shared secret setup** needed – public keys are fetched by alias.
- **No complex key exchange** for users – the server handles discovery, akin to how Signal or WhatsApp fetches keys from a server to initiate secure chats.
- **No user mistakes** like forgetting to encrypt or using the wrong key – the client app takes care of it and even signs everything to prevent human error.
- **Anonymity option** – unique among enterprise solutions, giving users control over how much identity to reveal.

## Market Opportunity and Timing

The timing for SurePack is ideal. **Secure file transfer is a growing market** and a pain point for many organizations. Multiple independent analyses show this market is already multi-billion dollar in size and rising steadily. For example, one report estimates the global secure file transfer market at **$2.4 billion in 2024** and projects it to reach about **$3.7 billion by 2033**. Another study projects an even faster growth trajectory – from ~$2.3 billion in 2023 to **over $5 billion by 2033** (8%+ CAGR). This growth is driven by the **urgent need for data protection** across all industries. As digital transformation and remote work expand the exchange of sensitive data, companies are investing in secure transfer solutions "to avoid data breaches and comply with privacy laws".

Importantly, **regulatory pressures are increasing**. Laws like the EU's GDPR, California's CCPA, HIPAA in healthcare, and Australia's own Privacy Act demand strict safeguarding of personal data in transit. Companies face heavy fines and legal penalties for exposing customer or confidential information. (GDPR, for instance, allows fines up to 4% of global turnover for serious violations.) According to market research, the rollout of privacy regulations worldwide has **pushed organizations to prioritize secure file transfer methods** to remain compliant. In Australia, the government passed the Cyber Security Act 2024, the first cybersecurity-specific law, signaling a regulatory push for better cyber hygiene. Businesses that proactively secure their file exchanges will not only avoid penalties but also build trust with clients who are increasingly concerned about privacy.

Additionally, high-profile data breaches and espionage cases have made **cybersecurity a boardroom issue**. Executives now recognize that insecure file sharing (e.g. emailing unencrypted spreadsheets or using personal Dropbox accounts) is a liability. In a recent survey, **68% of U.S. employees admitted to saving or deleting company information from IM apps on their own**, outside of official IT control – behavior that could lead

to compliance nightmares. Organizations are actively seeking solutions that **lock down file sharing without disrupting workflow**. SurePack fits this need perfectly: it gives employees an easy tool that actually enhances security **without forcing them to jump through hoops**. By embracing a solution like SurePack, a company can mitigate the human factor in data leaks (often cited as the weakest link in security) while enabling productivity.

On the technology front, the need for **post-quantum encryption** is emerging as a strategic concern. Government agencies and large enterprises are already planning upgrades to their cryptography, fearing a "harvest now, decrypt later" scenario where adversaries steal encrypted data today to decrypt in a decade. NIST's standardization of algorithms like Kyber in 2024 is a clear green light: organizations are **expected to start integrating PQC into products immediately**. In fact, global tech players have started doing so – e.g., Cloudflare's data shows significant adoption of PQC in web traffic. This is a **key timing advantage** for SurePack: we are delivering a solution that is *quantum-resilient from day one*. This can attract forward-looking customers (finance, government, defense, critical infrastructure) who are mandated to achieve quantum safety in the near term. It also future-proofs our product, giving it a longer market lifespan and differentiation against older solutions.

In short, the confluence of **market demand, regulatory drivers, and technological transition** creates a perfect storm that SurePack is positioned to capitalize on:

- **Large Market, Clear Need:** Organizations big and small need to send files securely; existing options are inadequate or too complex.
- **Growing Spend:** Cybersecurity spending is rising globally each year – secure communications are part of that budget. We only need a slice of this growing pie.
- **Management Awareness:** Cyber risk is now a C-suite and board concern, meaning willingness to invest in robust solutions is higher than ever (no longer an afterthought or just an "IT problem").
- **Lack of Easy Alternatives:** No mainstream product today offers the blend of anonymity, ease, and strong encryption that SurePack does. We would enter as one of the few modern options in a space dominated by legacy approaches.

## Competitive Advantages

SurePack stands out against both legacy solutions and current competitors:

- **Versus PGP and Email Encryption:** PGP has notoriously low adoption outside niche tech circles, due to poor usability and outdated design. Experts have documented PGP's myriad problems – from "absurd complexity" in its format to the lack of forward secrecy and reliance on long-term keys. Even modern email encryption efforts (S/MIME or PGP-based plugins) struggle with key distribution and user errors. SurePack eliminates these pain points. There is no key ring chaos, no manual exchange of public keys or signatures, and no risking that someone doesn't have the right plugin. By using a centralized lookup server for certificates (similar in spirit to how Let's Encrypt provides certificates automatically), SurePack **removes the friction** that stopped PGP from ever going mainstream. It's the **"no IT overhead" solution** – users don't need to be cryptography experts or hunt down each other's keys. Additionally, SurePack is built on modern encryption (AES-GCM, RSA-2048, SHA-512) with **no outdated ciphers**. As one blogger quipped, PGP is so old that if "Will Smith looked like this when your cryptography was current, you need better cryptography". We use **2020s crypto, not 1990s crypto**.

- **Versus Consumer File-Sharing (Dropbox, WeTransfer, etc.):** Typical file-sharing services prioritize convenience but **not end-to-end privacy**. They might encrypt data on the server, but the service can

still access your files (holding the keys), or the files are sent via just TLS and then stored unencrypted on the receiver's side. Those services also offer no sender authenticity guarantees or long-term confidentiality. In contrast, SurePack provides true **zero-knowledge file transfer** – even if a cloud storage provider or network is compromised, the attacker gets nothing useful. For industries like legal, healthcare, or finance dealing with confidential documents, this level of security is essential. Moreover, our solution can be self-hosted if needed (since it's based on ASP.NET Core and S3, a company could run their own instance for complete control). This appeals to enterprises with compliance requirements to keep data in-country or under specific governance.

- **Versus Enterprise Managed File Transfer (MFT) Solutions:** There are enterprise MFT and secure email gateway products (e.g. Kiteworks, Globalscape, Accellion). While they offer secure channels, they are typically **expensive, complex to deploy, and often not truly end-to-end** (they decrypt and re-encrypt data on servers for DLP scanning, etc.). Many require users to log into a web portal to retrieve files or have cumbersome password exchange for each file sent. SurePack's simplicity is a differentiator – it's more **agile and user-centric**. It can be rolled out without heavy infrastructure (the cloud server backend could even be offered by us as a service, lowering client IT burden). And unlike typical MFT, our **anonymous certificate model** means **built-in user privacy** – we don't force every user to be registered with personal details. This could be a selling point for journalists, NGOs, or any collaboration where participants need pseudonymity.

- **Uniquely Anonymous + Identity-Optional:** In today's world, providing privacy-preserving technology can be a market winner. Messaging apps like Signal gained adoption partly by **not requiring user identities beyond a phone number**. SurePack's ability to operate without tying files to explicit identities opens up use cases – from whistleblowing platforms to simply protecting employee privacy on internal communications. Yet, when identity is needed (say a law firm wants to know which attorney sent a file), the system supports it. This flexibility sets us apart: competitors either focus on anonymity (e.g. OnionShare for anonymous file sending over Tor) but lack enterprise manageability, or they focus on enterprise identity and forget privacy. SurePack uniquely **bridges that gap**, offering the option for either mode.

In summary, SurePack combines the security experts have long desired with the **usability that end users actually need**. As one cryptography professor noted, there is "so much potential in this area and so many opportunities to do better... it's time to stop looking backwards". SurePack *is* that better, forward-looking solution – delivering secure file sharing that is robust, easy, and ready for the threats of tomorrow.

## Execution Plan and Why We're Ready

Our team has not only envisioned this product – **we've built it.** The heavy R&D lifting (architecture design, cryptographic implementation, and prototyping) is already done and **validated in action**. We have a working codebase for both client and server. In fact, a reference implementation is live at **Suredrop.org**, demonstrating the technology in real-world conditions. This significantly de-risks the project: we are not asking for a leap of faith on unproven tech, but rather to productize and launch what we've already proven to work.

Key development milestones already achieved:

- **Core Cryptography:** The hybrid encryption and ACE certificate issuance flows are fully implemented and tested. We used well-known libraries (e.g. BouncyCastle for crypto, AWS SDK for storage) to avoid reinventing the wheel, following best practices in security coding. We have conducted internal code

reviews for security and even basic threat modeling (e.g. ensuring the server is hardened with rate limits to prevent abuse, using HTTPS everywhere, etc.).

- **Client Features:** The CLI tool supports all major functions (create keys, pack/unpack, send/receive, list, verify, delete). The GUI (built likely with .NET or Electron) provides a friendlier interface and is functional. This means we have a **ready-to-use product** that could be piloted with actual users very quickly.
- **Server & Cloud Infra:** The server is built on **ASP.NET Core**, known for its performance and reliability, and it's cloud-ready. We are using **Amazon S3 for storage**, which gives virtually infinite scalability and durability out-of-the-box. The server statelessly references S3 objects, so it can scale horizontally (behind a load balancer) if demand grows. We've also implemented measures like **encrypted storage for the root CA key** (protected with AES-GCM and a passphrase) and logging via Serilog for audit trails. The server APIs align with REST standards, making integration easy for other systems.

With the core built, **what remains is largely polish, packaging, and go-to-market execution** – areas where an investment can accelerate success:

- **Security Audit & Compliance:** Before commercial launch, we'd engage third-party experts to audit the cryptographic implementation and overall security (penetration test). Given the stakes (we are a security product), this due diligence will help convince skeptics (like our own boss, or future clients!) that SurePack is rock-solid. We may also pursue certifications (ISO 27001 for our processes, maybe Common Criteria or FIPS validation for our crypto modules) to ease adoption in sensitive industries.
- **User Experience & Integrations:** We plan to refine the GUI for a slick user experience and possibly develop plugins/integrations – e.g. an Outlook add-in to "Send Secure with SurePack" or a mobile app version for iOS/Android so files can be shared from phones. These will broaden the product appeal.
- **Business Model & Pricing:** We envision a **subscription model** (SaaS) for hosting on our SureDrop server cluster, as well as an enterprise licensing model for on-premise deployments. For instance, SMEs could pay a per-user or per-transfer fee to use our hosted service (much like Dropbox but secure), whereas a government department could license the software for a private deployment. The small size of files (thanks to compression and splitting) means even large transfers are efficient, and we could tier pricing by storage or bandwidth usage.
- **Market Entry:** With funding, we would execute targeted marketing to industries with acute needs: e.g. legal firms exchanging contracts, healthcare providers sending medical records, tech companies handling intellectual property, and defense/government communications. We can leverage case studies of recent breaches in these sectors to highlight how SurePack would mitigate those. Also, given our Australian base, we could align with the government's cybersecurity initiatives, potentially obtaining grants or partnerships (the Australian Cyber Strategy 2023 mentions supporting development of quantum-safe encryption – we fit that narrative well).

From an investment perspective, this is a compelling proposal because **much of the technical risk has been retired** by the work already completed. The funds would primarily fuel hardening the product and scaling it to market, rather than blue-sky research. Essentially, we have a **Formula 1 engine built and tested – now we need to put it in a sleek car and hit the track with a marketing strategy**. Our small size (<50 staff) is actually an advantage here: we can move fast and innovate without bureaucratic drag. Yet we also have the credibility of being a publicly listed ASX company, which can reassure enterprise customers that we're stable and accountable (something an open-source hobby project cannot as easily claim).

## Conclusion: A Timely Opportunity for Innovation and Growth

In conclusion, **SurePack represents a unique opportunity** for our company to launch a cutting-edge cybersecurity product at the exact moment the world needs it. It addresses a clear and growing pain point with a solution that is technically advanced but user-centric. All the trends – remote collaboration, stricter privacy laws, rising cyberattacks, the coming post-quantum revolution – point toward a surging demand for exactly this kind of secure file sharing capability.

We have in our hands a working, innovative platform that **outshines legacy solutions** (as evidenced by expert criticisms of those tools) and offers concrete, fact-based advantages. Our approach is backed by defensible stats and standards: global surveys show the need for better security practices, market research shows organizations are investing more in secure file transfer, and government bodies like NIST are urging immediate adoption of the very cryptography we've built in. This gives us powerful talking points for customers and a head start on any competitors still playing catch-up.

For our company, investing in SurePack's productization and go-to-market is an opportunity to **diversify and innovate** with a solution that could generate new revenue streams. Given that we recently capitalized from a business sale and are actively looking for R&D investments, SurePack fits perfectly: it leverages our team's expertise, has global market potential, and could position us as leaders in a niche that aligns with the future of cybersecurity. The upside is significant – even capturing a small fraction of a multi-billion dollar market would yield substantial returns – and the downside is minimized by the progress already made.

Our boss may be a cynic, but the facts are on our side. **Secure, anonymous, quantum-ready file sharing** is not science fiction; it's running today in SurePack, and the world is asking for it. By supporting this initiative, we can transform a homegrown innovation into a commercial success that puts us at the forefront of secure communication technology. Let's seize this chance to turn SurePack into the next big product for our company – the right solution at the right time, with the right team to deliver it.

**Sources:**


- Latacora, *"The PGP Problem,"* 2019.
- M. Green, *"What's the matter with PGP?"* A Few Thoughts on Cryptographic Engineering, 2014.
- Veritas, *"The Hidden Threat of Business Collaboration"* (Data Sharing Survey), 2021.
- IBM Security, *Cost of a Data Breach Report 2024* (TechRepublic summary).
- IMARC Group, *Secure File Transfer Market Report 2025-2033*, 2024.
- Market.us, *Secure File Transfer Market Analysis*, Mar 2025.
- NIST, *Post-Quantum Cryptography Standards Announcement*, Aug 2024.
- The Register, *"Cloudflare 2024 Year in Review,"* Dec 2024.