> “The enterprise has full control of what files are shared, who they are shared with, and the level of security for each file and user.”

KRYPDOX

ULTRA-SECURE ENTERPRISE MOBILE FILE DISTRIBUTION

Business class file sharing services provide adequate security for most documents, but there are sensitive materials that demand a higher level of protection. That’s why we created Krypdox. It protects against the four main vectors of a security threat:

Device Theft. Millions of smartphones and tablets are lost or stolen each year. A savvy thief can hack their way past standard security in just minutes. Krypdox uses multiple layers of security to ensure that files cannot be accessed, even by the most sophisticated hacker. Enterprises can completely revoke access on a per user or per device basis.

User Theft and Circumvention. Most security breaches come from authorized users sharing information with others. This happens intentionally or through social hacking schemes. Krypdox does not allow users to share, export or print documents.

Network Hack. All data between the user’s device and the Krypdox servers are transmitted over an encrypted channel with mutual authentication. This ensures that only the intended recipient can access the information. Inside this encrypted channel, each message packet is uniquely encrypted, providing another layer of protection.

Server Hack. Krypdox is built on a distributed architecture that keeps all unencrypted data behind the corporate firewall. Encrypted documents are stored in the cloud and can only be decrypted on authorized devices.

A TRUE ENTERPRISE SOLUTION

Unlike peer-to-peer file sharing applications such as DropBox, the enterprise has full control of what files are shared, who they are shared with, and the level of security for each particular file and user.

Audit logs capture viewing history and timestamps. Files can be deleted remotely. Multi-layer security ensures that even if one encryption mechanism is broken, the data is still secured by a second layer.

Krypdox provides the highest level of protection for files that must absolutely remain confidential, such as:

- Pre-release film and dailies
- Financial reports
- Lab notebooks
- Trade secrets
- Healthcare data, PHI

Krypdox is delivered as a turnkey server and application solution that can run from a commercial cloud such as Amazon AWS. The platform is OS and device agnostic. Krypdox for iPad is available now. Android, Windows and OS X clients are planned for future releases.

For more information contact sales@asynchrony.com.

asynchrony
900 Spruce Street, Suite 700 • Saint Louis, Mo. 63102
314.678.2200

KRYPDOX

MULTIPLE LAYERS OF SECURITY

- **User Roles** - Multiple roles for access to different functionality in the network. Security officers can audit files and manage users and devices. Content owners can upload files.
- **iPad Strong PIN** - The user must enter their PIN any time they re-enter the iPad app. Strong PIN detection ensures an appropriate strength PIN is chosen. The PIN is never stored on the iPad and must be entered to unlock all of the encrypted data.
- **LDAP Integration** - User roles are defined in LDAP. Authentication integrates with LDAP.
- **Document Encryption** - All documents are encrypted with an AES 256-bit symmetric key.
- **Per-User Document Key Encryption** - All document keys are encrypted separately for each authorized user with an Elliptic Curve Integrated Encryption Scheme.
- **TLS** - All communications traffic between the iPad and ionic mobile servers are encrypted over a TLS connection using 2048-bit RSA keys and a 384-bit EC key with group secp384r1 Diffie Hellman key exchange.
- **Server Enclave** - The Master server lives behind the corporate firewall and is responsible for encrypting all documents and pushing them to one or more Child servers that live in the cloud. Encrypted documents can only be decrypted by properly permissioned and authorized devices. Unencrypted data is never stored in the cloud.
- **Maximum Saved Documents** - Each iPad user can be assigned a quota of saved documents on the iPad. This limits exposure in the event of a stolen iPad.
- **Maximum Document Upload** - Each content owner can be assigned a maximum number of documents that can live on the system at any given time.
- **Document Classification** - Configurable list of document classifications, e.g Confidential, Classified, Secret, Top Secret.
- **Time to Live (TTL)-** Saved documents on the iPad are assigned a time to live. When the TTL expires, the document key is deleted from the iPad, rendering the document useless.
- **Certificate Revocation** - Security officers can revoke iPad certificates, rendering the iPad incapable of communicating with the server.

ABOUT ASYNCHRONY

Asynchrony has been helping organizations with Enterprise Mobility for over a decade, since the days of the Palm Pilot and Pocket PC. Most recently, we've been creating custom iOS and Android apps for some of the most progressive companies in their industries, including healthcare, financial services, retail, electronics, public safety and defense.

Asynchrony also helps companies develop unified mobility strategies and the supporting resources needed to achieve them, including the establishment of *Mobile Centers of Excellence*. This ensures that our clients deploy mobility solutions that are integrated, usable, scalable and secure.

In addition to mobile products, Asynchrony develops software solutions ranging from back-end government middleware to front-end applications and full-scale, commercial cloud infrastructures. In short, Asynchrony connects people, sensors, information and systems.

The Asynchrony team is comprised of highly-motivated experts focused on developing well-designed, usable software backed by hard-core tech and engineering.

For more information, contact:
sales@asynchrony.com

asynchrony

900 Spruce Street, Suite 700 • Saint Louis, Mo. 63102
314.678.2200