QWANTUM private messaging

VISIONARY AWARD 2022

Qwantum Private Messaging

Privacy | Integrity | Authenticity

Product Features

- Hardened Encryption
- Secure Tokenization
- Physical Authentication
- No Username and Password
- No Database
- Encryption Keys are Never Stored
- Nothing to Steal

Qwantum Access Card and Reader - Gliding the card authenticates your access and generates unique encryption keys with every transaction.

Privacy as a Service

Qwantum™ Private Messaging is an app that delivers "Privacy as a Service" to its Club Members. This powerful new service of MagTek, lets you use public communication channels or storage systems to send or save sensitive material simply and quickly by privatizing the material first. And we do not trust Usernames and Passwords for security. We do employ a hard token (the Qwantum Card) that generates a derivative, unique Qwantum one-time token with every use. The form-factor is a metal card. It identifies you as a member of the Qwantum Club, is counterfeit resistant and tamper responsive, and it initiates a process to create a unique AES 256 encryption key, used exclusively to privatize your messages and files. QPM is not bio-intrusive. It does not need your face, fingerprints, voice, DNA, or any personal data in order to operate.

MagTek has solved the problem of secure key exchange between designated parties using a powerful combination of physical token authentication and the generation of a unique encryption key per transaction, whereby the parties do not need to know or transport the secret keys.

The keys are generated inside a host security module, where they encrypt, or decrypt data inside as needed. The keys are generated in real time, are zeroed out after use, and are never stored in MagTek databases. The secret keys are generated in conjunction with the physical authentication of a Qwantum Card, a specific transaction, and the transaction's authorized endpoints (the Qwantum Club users). The system truly bridges the physical world with the digital world, protecting both the ingredients and the recipe used to build encryption security. Without access to the physical aspect of the Qwantum Card and its unique per transaction authentication data, quantum computing attacks, as they are currently theorized, cannot succeed against Qwantum Private Messaging.

CALL - 562.546.6400 | EMAIL - QwantumMediaSales@magtek.com

Qwantum PM Use Cases

- **Save a Tree.** Save Money on Overnight Shipping. When you absolutely, positively need to get it there safely, in minutes, use Qwantum Private Messaging.
- **Cryptocurrency Wallet Passwords.** To protect extremely long and complex passwords for on-line or off-line storage. Don't be the person to lose millions of dollars because you forgot your password, or you don't want to save it anywhere in-the-clear!
- **Cloud Document Storage.** Think twice and protect yourself before you drop that document on Dropbox, Adobe, Google, Apple, Azure or other on-line storage facility.
- **Secure Distribution** of Subscription-based e-Newsletters and Periodicals. Ensure that the subscription information can only be viewed by intended parties.
- **Human Resources.** To protect Personally Identifiable Data (PII), HIPAA information, personnel files, etc. IT professionals cannot access private information. It is for HR's eyes only!
- **Legal Documents.** To protect contracts, last will and testaments, digital passports, birth certificates, intellectual property, formulae, negotiation terms and conditions, legal briefs, merger and acquisition plans. Negotiations can remain secret.
- **Medical Information**. To protect lab results or other personal medical information. Medical professionals can now share private info over public communications channels.
- **Financial Information.** To protect corporate earnings, business proposals, initial public offerings of stocks and equities, projections, and forecasts. Share information without fear of it being accidentally breached.
- **Banking Information.** Wire transfer information, Disputes, Digital Card Data. Financial institutions can now share private or sensitive data with their consumers and utilize File Signatures to verify and validate the integrity of the communication.
- **High net worth clients.** Private chat, social media invitations, communications, passwords, and other sensitive data. Imagine a celebrity inviting. Club Members to a private event, but using Social Media to get the word out, privately but publicly.
- **Secure Communications** with Family and Friends. You have a right to privacy. Defend it. Protect it.

Nothing Stored, Nothing to Steal

Qwantum Private Messaging does NOT store anything about your Private Messages. There are no usernames and passwords. The encryption keys are unique to each message and never in the clear. The Private Messages are not stored in our databases. We developed Qwantum Private Messaging with your privacy in mind. Distributing the data and deliberately not storing it in a central repository makes it very unattractive for bad actors to commit data theft.

Qwantum Club Membership

As a Qwantum Club Member, you will receive a Qwantum Card, a Qwantum Reader and a Membership to the Qwantum Club. This will give you complete access to all Qwantum Private Messaging functions and services. If you want to share Qwantum Private Messages with Non-Club Members, just create Qwantum Access Tokens and share them with your trusted parties. It is like sharing a house key or door code without fear that anyone can duplicate the key or change the code without your permission. Qwantum Access Tokens are safe to use and you can revoke them at any time, so you never have to worry about unwanted or unauthorized access.

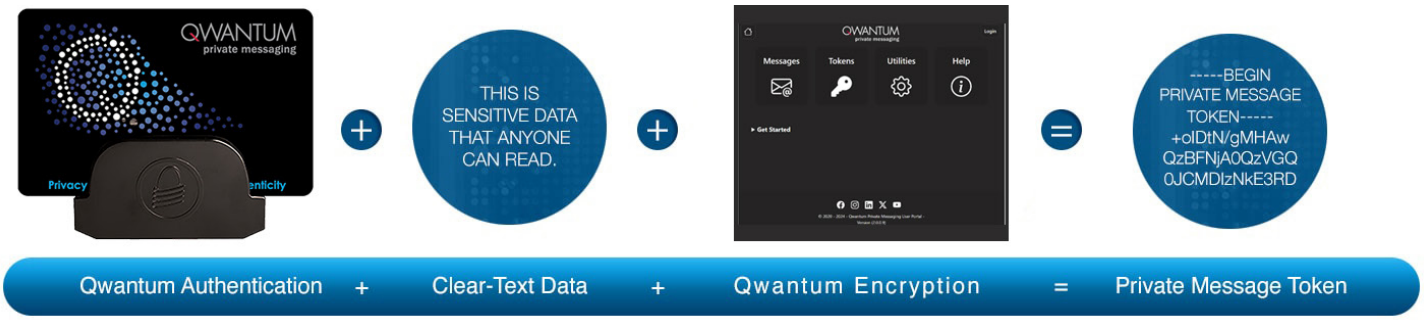
Compatibility

Operating Systems

Windows
iOS
Mac
Android
Linux

Browser Options

MagneFlex by MagTek
Chrome
DuckDuckGo
Safari
Firefox
Internet Explorer
Opera
and more



MAGTEK®
SECURITY FROM THE INSIDE

Celebrating 50 years! Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission and security of cards, barcodes, checks, PINs and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Its products include secure card reader/authenticators, Qwantum secure cards, token generators, EMV contact, contactless, barcode and NFC reading devices, encrypting check scanners, PIN pads and distributed credential personalization systems for secure magstripe and EMV enabled cards. These products are used worldwide by financial institutions, retailers, payment processors, and ISVs to provide secure and efficient data privacy, as well as payment and identification transactions. Today, MagTek continues to innovate. Its MagneSafe® Security Architecture leverages strong encryption, secure tokenization, dynamic card authentication, and device/host validation enabling users to assess the trustworthiness of credentials and terminals used for online identification, payment processing, and high-value electronic transactions. MagTek is headquartered in Seal Beach, CA.