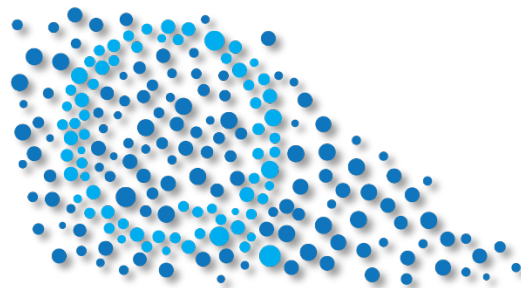


Qwantum Private Messaging

Use Cases

Overview and Operation



June 2022

Document Number:
D998200528-10

REGISTERED TO ISO 9001:2015

Copyright © 2006 - 2022 MagTek, Inc.
Printed in the United States of America

INFORMATION IN THIS PUBLICATION IS SUBJECT TO CHANGE WITHOUT NOTICE AND MAY CONTAIN TECHNICAL INACCURACIES OR GRAPHICAL DISCREPANCIES. CHANGES OR IMPROVEMENTS MADE TO THIS PRODUCT WILL BE UPDATED IN THE NEXT PUBLICATION RELEASE. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT THE EXPRESS WRITTEN PERMISSION OF MAGTEK, INC.

MagTek®, MagnePrint®, and MagneSafe® are registered trademarks of MagTek, Inc. Magensa™ is a trademark of MagTek, Inc.

ANSI®, the ANSI logo, and numerous other identifiers containing "ANSI" are registered trademarks, service marks, and accreditation marks of the American National Standards Institute (ANSI).

ISO® is a registered trademark of the International Organization for Standardization.

UL™ and the UL logo are trademarks of UL LLC.

PCI Security Standards Council® is a registered trademark of the PCI Security Standards Council, LLC.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere.

The EMV trademark is owned by EMVCo, LLC. The Contactless Indicator mark, consisting of four graduating arcs, is a trademark owned by and used with permission of EMVCo, LLC.

The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by MagTek is under license.

Google Play™ store, Google Wallet™ payment service, and Android™ platform are trademarks of Google Inc.

Apple Pay®, iPhone®, iPod®, Mac®, and OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries. iPad™ is a trademark of Apple, Inc. App StoreSM is a service mark of Apple Inc., registered in the U.S. and other countries. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple Inc. under license.

Microsoft®, Windows®, and .NET® are registered trademarks of Microsoft Corporation.

All other system names and product names are the property of their respective owners.

Table 0-1 - Revisions

Rev Number	Date	Notes
10	June 2022	Initial Release

SOFTWARE LICENSE AGREEMENT

IMPORTANT: YOU SHOULD CAREFULLY READ ALL THE TERMS, CONDITIONS AND RESTRICTIONS OF THIS LICENSE AGREEMENT BEFORE INSTALLING THE SOFTWARE PACKAGE. YOUR INSTALLATION OF THE SOFTWARE PACKAGE PRESUMES YOUR ACCEPTANCE OF THE TERMS, CONDITIONS, AND RESTRICTIONS CONTAINED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, CONDITIONS, AND RESTRICTIONS, PROMPTLY RETURN THE SOFTWARE PACKAGE AND ASSOCIATED DOCUMENTATION TO THE ADDRESS ON THE FRONT PAGE OF THIS DOCUMENT, ATTENTION: CUSTOMER SUPPORT.

TERMS, CONDITIONS, AND RESTRICTIONS

MagTek, Incorporated (the "Licensor") owns and has the right to distribute the described software and documentation, collectively referred to as the "Software."

LICENSE: Licensor grants you (the "Licensee") the right to use the Software in conjunction with MagTek products. LICENSEE MAY NOT COPY, MODIFY, OR TRANSFER THE SOFTWARE IN WHOLE OR IN PART EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. Licensee may not decompile, disassemble, or in any other manner attempt to reverse engineer the Software. Licensee shall not tamper with, bypass, or alter any security features of the software or attempt to do so.

TRANSFER: Licensee may not transfer the Software or license to the Software to another party without the prior written authorization of the Licensor. If Licensee transfers the Software without authorization, all rights granted under this Agreement are automatically terminated.

COPYRIGHT: The Software is copyrighted. Licensee may not copy the Software except for archival purposes or to load for execution purposes. All other copies of the Software are in violation of this Agreement.

TERM: This Agreement is in effect as long as Licensee continues the use of the Software. The Licensor also reserves the right to terminate this Agreement if Licensee fails to comply with any of the terms, conditions, or restrictions contained herein. Should Licensor terminate this Agreement due to Licensee's failure to comply, Licensee agrees to return the Software to Licensor. Receipt of returned Software by the Licensor shall mark the termination.

LIMITED WARRANTY: Licensor warrants to the Licensee that the disk(s) or other media on which the Software is recorded are free from defects in material or workmanship under normal use.

THE SOFTWARE IS PROVIDED AS IS. LICENSOR MAKES NO OTHER WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Because of the diversity of conditions and PC hardware under which the Software may be used, Licensor does not warrant that the Software will meet Licensee specifications or that the operation of the Software will be uninterrupted or free of errors.

IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE, OR INABILITY TO USE, THE SOFTWARE. Licensee's sole remedy in the event of a defect in material or workmanship is expressly limited to replacement of the Software disk(s) if applicable.

GOVERNING LAW: If any provision of this Agreement is found to be unlawful, void, or unenforceable, that provision shall be removed from consideration under this Agreement and will not affect the enforceability of any of the remaining provisions. This Agreement shall be governed by the laws of the State of California and shall inure to the benefit of MagTek, Incorporated, its successors or assigns.

ACKNOWLEDGMENT: LICENSEE ACKNOWLEDGES THAT HE HAS READ THIS AGREEMENT, UNDERSTANDS ALL OF ITS TERMS, CONDITIONS, AND RESTRICTIONS, AND AGREES TO BE BOUND BY THEM. LICENSEE ALSO AGREES THAT THIS AGREEMENT SUPERSEDES ANY AND ALL VERBAL AND WRITTEN COMMUNICATIONS BETWEEN LICENSOR AND LICENSEE OR THEIR ASSIGNS RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

QUESTIONS REGARDING THIS AGREEMENT SHOULD BE ADDRESSED IN WRITING TO MAGTEK, INCORPORATED, ATTENTION: CUSTOMER SUPPORT, AT THE ADDRESS LISTED IN THIS DOCUMENT, OR E-MAILED TO SUPPORT@MAGTEK.COM.

Table of Contents

SOFTWARE LICENSE AGREEMENT	4
Table of Contents	6
1 Our Vision	7
2 Why Use Qwantum Private Messaging?	7
3 Save Money on Overnight Shipping	8
4 Keep HR Information CONFIDENTIAL	9
4.1 Employment Agreements	9
4.2 Incident Reports	9
5 Financial Institutions – Account Opening Documents	9
6 Other Uses	10
7 Qwantum Cardware	11
8 Join The Club!	12
9 Technical Specifications	12

1 Our Vision

“The right of the people to be secure in their persons, houses, papers, and effects...”
(From the 4th Amendment of the Bill of Rights to the United States Constitution).

Those few words say it all.

People have a fundamental right to privacy.

They should be free to communicate with one another and have confidence that their communications are secure, private, and only shared with intended parties.

At **Qwantum Private Messaging**, our core **vision** is the belief that all people have a fundamental right to private electronic communications and data. To that end, we have developed a “Privacy as a Service” secure messaging platform that adheres to the fundamental principles of “Privacy”, “Integrity”, and “Authenticity”.

With Qwantum Private Messaging you are assured that any messages you create will remain cryptographically secure, authenticated, and private.

2 Why Use Qwantum Private Messaging?

Club Members can use the application to encrypt almost any kind of data. The encrypted data can be saved to a file and stored locally, in the cloud, or in the Apple Wallet, wherever you choose. You can also redact, encrypt and replace sensitive data within a form or document. The Qwantum Private Messaging service can also send the encrypted data directly to your designated recipients by email. This powerfully secure service gives you the privacy and peace of mind you deserve with the convenience you need.

Qwantum Private Messaging can be used everywhere you have access to the Internet. It can be used with any operating system and any browser. It can be used on your mobile phone, tablet, or computer. If you value privacy, integrity, and authenticity, become a Qwantum Club Member, and protect your data now.

The rest of this document will describe use cases for Qwantum Private Messaging.

3 Save Money on Overnight Shipping

When you absolutely, positively need to get it there safely, **in minutes**, use *Qwantum Private Messaging*

- An M&A firm in Boston wants to send a proposal about a prospective acquisition to a firm in Pennsylvania.
- A trendy, upscale Retailer wants to send confidential design files to a manufacturer regarding next season’s look
- A CFO wants to send corporate Financial Statements to the executive team for tomorrow’s Zoom meeting

	Overnight Delivery Service	Qwantum Private Messaging
Transit Time	12 hours minimum	5 minutes
Proof of Delivery	Yes – when requested	Yes, Automatic
Read Receipts	No	Yes, per Recipient
Location at Read event	No	Yes, if specified
Multiple, Simultaneous Destinations	No	Yes
Paper Savings	No	Yes
Price	\$\$\$	\$
Overnight Envelope 1 lb. 10:30 am	\$46.80	\$12.50*
Overnight Envelope 1 lb. 8:30 am	\$92.80	\$5.00**
*Based on 2 shipments per week		
**Based on 5 shipments per week		

Roll over your rate quote for a breakdown of costs.
Amounts are shown in USD

Select	Service and Transit Time	Your Rate
<input type="radio"/>	FedEx Priority Overnight® 10:30 am Wed Mar 02, 2022	<u>46.80</u>
<input type="radio"/>	FedEx Express Saver® 04:30 pm Fri Mar 04, 2022	<u>10.45</u>
<input type="radio"/>	FedEx 2Day AM® 10:30 am Thu Mar 03, 2022	<u>29.05</u>
<input checked="" type="radio"/>	FedEx First Overnight® 08:30 am Wed Mar 02, 2022	<u>92.80</u>

4 Keep HR Information CONFIDENTIAL

4.1 Employment Agreements

A new employee must submit a signed employment agreement which includes her Date of Birth, Social Security Number, and two forms of government issued Identification. She will be working remotely and therefor unavailable to bring the information in person on her first day of employment.

Instead, the HR manager sends her a Guest Token to the QPM site. The employee fills out the form, signs where necessary and takes a photograph of the 2 forms of identification and appends it to the HR Form. She then goes to the QMP site where her guest token has been pre-loaded and encrypts the document. It is then automatically emailed to the HR Manager. The new employee cannot change the email address of the HR Manager, and only the HR manager can decrypt it.

When the HR manager receives the form from the new employee, she views it and can store it encrypted in the appropriate HR folder.

Then, the HR manager will send the new employee her company credentials (ID Number, Username and Password). The HR manager can follow that up with a 10-day Guest Token the new employee can use whenever she needs to retrieve the sensitive data.

4.2 Incident Reports

The HR manager received a visit this morning from a very distraught employee. The employee reported that he had been physically and sexually accosted by an on-premises contractor. The HR manager took a report in which many disturbing and potentially embarrassing details were included. The HR manager contacted the police and then immediately encrypted the report before storing it in the HR Incident Report folder.

The HR department routinely fields questions and provides information about what is covered by the company's Health Insurance policies. Much of this information is sensitive and covered by the HIPAA regulations for the protection of EPHI or Electronic Personal Health Information. The HR department had been using a designated area of the corporate network that was managed by IT and controlled by Username and Password. Now that the HR department uses Quantum Private Messaging, it can encrypt any file deemed sensitive and contain that data for HR eyes only.

5 Financial Institutions – Account Opening Documents

A wealthy Account Holder at a large national bank has recently passed away and the Attorney for her estate has an upcoming meeting with her Bank Representative regarding the closing of certain accounts, the renaming of certain accounts, the opening of new accounts, address changes, signature card updates etc.

The Banker has asked the attorney for a list of items that he will need to make these adjustments. Among them are: The Death Certificate, the existing Trust Documents, the Durable Power of Attorney (DPOA), the new Trust Documents, Court Orders, the deceased's Social Security number, and any new EINs. Each of these documents will need to be reviewed by the central office. Ordinarily, the documents are sent by facsimile to the central review center. The fax machine is an ordinary one. There is no encryption or special security measures. In the minds of many, the fax is used because "It's safer than the internet."

Now that QPM is available to transmit these documents, the queue at the fax machine is unnecessary. The documents can be encrypted and emailed from the computer at the service representative's desk. At central review the documents can be deciphered and viewed (no paper printouts needed) and filed electronically encrypted or in the clear per the Bank's policy. The Bank Account Representative and the Account holder have a quicker, safer, and less-hassle experience.

6 Other Uses

Cryptocurrency Wallet Passwords. To protect extremely long and complex passwords for online or offline 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 online 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!

Celebrities and other 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.

7 Quantum Cardware

No PANs, No Names, Only Tokens, Multiple Functions

What makes Quantum Private Messaging so extraordinary? It's the Quantum Card. Your unique, unclonable, metal Quantum card is the crucial element to privatize your messages and data files. Without the Quantum card, the data cannot be enciphered. Without the Quantum card data cannot be deciphered or viewed. Your Quantum Card outputs only tokens. The first part of the token is static, while the second part is a long, dynamic, complicated, digital string that changes with every use. Just the act of touching or tapping the card causes the token to morph. Much like a kaleidoscope, the colorful crystals do not change and remain identifiable but tapping the scope ever so gently changes the light, refractions, color, size and patterns rendered to the viewer. The motion of the materials results in an ever-changing view being presented. This is just what happens with a Quantum Authentication Token. The digital pattern is always changing.

If you were to view the token on the Quantum stripe, you would see that there is no sensitive data there. There are no account numbers, no names, no expiration dates, like those on a traditional card. There is only a token which is a substitute for the born-on date (down to the second) of the Quantum card.



This ensures no two Quantum cards have an identical static part of the token, and a lookup of the token can confirm when and where it was produced. Next you will see the enciphered dynamic part of the token. This string of data looks like gibberish, but it's the piece of the token the Quantum engine will use to ascertain that the card is unaltered and authentic. Once this string of gibberish has been deciphered and authenticated, some zero and one bits will be selected as fodder for the key generation engine. This engine has several sources of fuel and a number of spark plugs. When the engine starts up it produces a unique AES 256 Key which is passed to the crypto block of the HSM and used to privatize or de-privatize the data. After each use they are zeroized. The AES 256 Keys are never stored in the HSM or anywhere at QPM. The enciphered Quantum Authentication Token is returned to you encapsulated in the Message token. You keep the essential ingredients and QPM keeps the recipe. You retain the crucial elements, but you do not need to see them, transport them, or disclose them to anyone. When you glide your Quantum card, and it is authenticated you authorize QPM to generate or regenerate an AES 256 Key that will be used to protect or view a message. That key is known temporarily and only by the Host Security Module. If you do not provide the authentication token to QPM, the HSM has no means to generate the key or decipher the data. With your Quantum card in hand, you are always and exclusively in control of your protected messages and files.

8 Join The Club!

To become a Quantum Club Member, you can sign up [here](#). You will receive a Quantum Card, a Quantum Reader and a 3-month Membership to the Quantum Club. This will give you complete access to all Quantum Private Messaging functions and services. If you want to share Quantum Private Messages with Non-Club Members, just create Quantum Guest 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. Quantum Guest Tokens are safe to use, and you can revoke them at any time, so you never have to worry about unwanted or unauthorized access.

9 Technical Specifications

Technical Specifications
AES Encryption