# Authentication- The Basis of Trust

*MagTek, a reputation built on trust. Trust, built on the ability to authenticate.*

White Paper

March 2022

Document Number:
D998200530-10

REGISTERED TO ISO 9001:2015

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. SOME FEATURES AND FUNCTIONS MAY BE DOCUMENTED, BUT NOT AVAILABLE WITH THE CURRENT RELEASE OF THE PRODUCT. PLEASE CONTACT YOUR MAGTEK REPRESENTATIVE FOR QUESTIONS ABOUT SPECIFIC FEATURES AND FUNCTIONS AND WHEN THEY ARE SCHEDULED TO BECOME AVAILABLE.

MagTek®, MagnePrint®, and MagneSafe® are registered trademarks of MagTek, Inc.
Magensa™ is a trademark of MagTek, Inc.
DynaPro™ and DynaPro Mini™, are trademarks of MagTek, Inc.
ExpressCard 2000™ is a trademark of MagTek, Inc.
IPAD® is a trademark of MagTek, Inc.
IntelliStripe® is a registered trademark of MagTek, Inc.

American Express® and EXPRESSPAY FROM AMERICAN EXPRESS® are registered trademarks of American Express Marketing & Development Corp.
D-PAYMENT APPLICATION SPECIFICATION® is a registered trademark to Discover Financial Services CORPORATION
MasterCard® is a registered trademark and PayPass™ and Tap & Go™ are trademarks of MasterCard International Incorporated.
Visa® and Visa payWave® are registered trademarks of Visa International Service Association.

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 Store$^{SM}$ 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 | 3/15/22 | Initial Release |

# Table of Contents

# 1 Thesis

If it can’t be authenticated, it can’t be trusted!

In any financial transaction system, you want to know with a high degree of certainty who you’re dealing with, how your privacy is protected, where the money is coming from and going to, how much is at stake, and what’s your recourse if something unexpected occurs.  In short, you want to trust the system. How can trust be established? At MagTek we believe its by a combination of things, including cryptography, tokenization, and authentication, which happens to be the strongest of them all.

# 2 Authentication versus Authorization.

Every payment system relies a great deal on its authorization network. But at MagTek, we emphasize the need for authentication to augment authorization. What is meant by the term authentication and how does it differ from authorization? Authentication is the act of measuring, proving or asserting genuineness. It answers the questions – is it real, is it true, is it valid, or is it genuine? Authorization is the granting of approval. Yes, I give my consent to move value, or no, I do not. It's binary. Yes or No. But if we were to rely solely on authorization, all kinds of fraud could occur. Let's look at our current Payment System for analysis. In a payment transaction, authorization is a must, but there are at least seven (7) elements that should be authenticated as well. Why? Because it's not enough to just approve a payment. Nor is it sufficient to just encrypt the payment data. Encryption scrambles valid data and counterfeit or fraudulent data equally well. And tokens are great, but not a silver bullet. A combination of security measures is required to make sure a payment transaction is safe and sound. So let's take a look at what should be authenticated, because even if it's "approved," if you can't authenticate it, you can't trust it.

## 2.1 The Parties.

This is usually the Payor and the Payee. Each party needs to trust the other. By an authentication process one must establish exactly who initiated the payment and is a party to it, as well as exact information about the recipient of the funds. This can be accomplished by authenticating appropriate credentials. Credentials fall into three categories, something the user has, knows or is. The user may present a physical token, biometric data, knowledge, a shared secret, or some combination of these things. We use presented credentials to authenticate the users – meaning if the credentials are valid, we are satisfied that both parties are who they say they are.

## 2.2 The Terminal.

The Terminal or Device that is used to conduct the transaction. This information is necessary and must be authenticated so that a relying Party can recognize if a clone or altered device has been inserted into the mix to harvest payment data or redirect it to unauthorized parties. Terminals these days, come in all shapes and sizes. Even a tablet or a mobile phone can be a payment device. This variety makes authentication even more difficult, but necessary.

## 2.3 The Credentials.

A physical credential, if used, should be authenticated such that the relying party can know that it is genuine and has not been altered. The physical token often identifies both the User and the Account. PINs, Passwords and biometric data are included here too. The greater the number and type of credentials presented and verified, the more likely the correct User is participating in the transaction.

## 2.4 The Accounts.

To start, the account where the funds currently reside. This could be a bank account, a line of credit, a crypto fund, or an escrow account. In a trustable transaction, the account should be authenticated so that one knows it is legitimate. And the same goes for the account into which the funds will move. This information should remain a verifiable part of the transaction record.

## 2.5 The Goods.

The goods and/or services to be exchanged. Here, sometimes the physical goods can be authenticated so that the true value of the transaction can be established. A genuine Rolex watch is much more valuable than a good knock off, but without an authentication process, value can be arbitrary.

## 2.6 The Authorization System.

The Authorization system and all its mid points. Who's is seeing the data, who is processing that data? Are they the rightful parties? All of the end-points and the mid-points should be able to prove who they are and why they need access to that data. The relying parties need to be able to trust the network, so an authentication system is essential.

## 2.7 The Amounts.

The currency type and amounts contained in the transaction. The devil is in the details. If the transaction was intended to be for $100, but actually is processed for $1,000, one party will suffer. One bad zero or a misplaced decimal point can make the transaction chaotic and difficult to unravel.

At MagTek, our objective is to build trustable transactions. Our methods vary, but the basic premise never changes. To trust a transaction, you must be able to authenticate its elements. Here is a sampling of the methods whereby we can authenticate a transaction.

# 3 The Methods

## 3.1 Physical Tokens.

Physical Tokens, such as cards, fobs, or phones need to be authenticated. At MagTek we can authenticate all sorts of tokens, based on intrinsic or dynamic data. Our Qwantum card technology is a good example. It identifies cards that have been counterfeited or altered, and thereby provides real-time data to deny authorization. Qwantum cards are safer and more durable than chip cards. They are also easier to use and cost half as much.

## 3.2 Hash Values.

Hash Values are one way derived digital numbers and letters that when replicated using the original data, a strong algorithm, and some salt and pepper (instead of keys) can mathematically prove that the data has not been altered or transformed.

## 3.3 One-time Codes.

One-time codes are powerful. We use them for lots of things. Because they are neither predictable nor reusable, their use in a transaction prevents disputes, and because they are not sensitive, they can live in a database in clear text.

## 3.4 Virtual Tokens.

Virtual Tokens can be likened to physical tokens. They are dynamic packets that will score high in the authentication engine, but no two will ever be identical. Static Virtual Tokens can be used as a substitute for sensitive data, like account numbers.

## 3.5 Challenge/Response.

Challenge/Response is a cryptographic function, whereby one party issues a challenge or a nonce, the other party encrypts the nonce with a shared key and returns the encrypted result. If the challenger can successfully decrypt the nonce, she can trust that the correct party received the nonce, used the correct key, and returned a valid response, hence the parties can proceed with the transaction, because mutual authentication has occurred.

## 3.6 Encryption/Decryption with DUKPT.

Encryption/Decryption can be used to authenticate as well as protect sensitive data. When a derived unique key per transaction (DUKPT) key management scheme is used, automatic authentication occurs. If any part of the message or key serial number (KSN) has been modified, it will fail encryption and result in gibberish. If the data is decrypted successfully, it could only have been encrypted by the unique device that contained the diversified starting key.

## 3.7 Replay checking.

There are circumstances where replay is allowed, but in most authentication systems, a transaction identical to a previous one is considered fraudulent or an error. Either way, it should be blocked. One method we use to detect and prevent replay is based on the Key Serial Number (KSN). We track the KSNs and once used we flag them as invalid for further use. We also use pattern matching to guard against replay. Once the authentication data has been decrypted, we check the database for identical authentication values as a second means to rule out a replay attack.

## 3.8 Message Authentication Codes.

Message Authentication Codes or MACs for short, establish that the message has not been altered, and that the two parties on either end of the channel have both used a shared secret.

## 3.9 Correlation Algorithms.

Correlation is a powerful tool. In authentication systems, many rely on binary validation. Yes, the PIN matches 100% or no, it does not. It’s pass/fail, Go/No go, or true/false. The difficulty with binary authentication methods is the static nature of the proof. Static results can be readily compromised. If your PIN or Password is discovered, an adversary can use it over and over again, until you realize it has been compromised and change it. With a correlation authentication scheme, we use statistics to measure the relationship between what is presented during the transaction and one or more stored authentication values. This allows us to accept dynamic, one-time use data as input. If an adversary were to discover the dynamic data presented at the transaction, it does not serve his purpose. If it is re-presented, we know it is replay and will decline the transaction. If it is a 100% match with a stored authentication value, it will also be declined, because the statistical model informs us the probability of a perfect score is so low, it can be presumed to be fraudulent.

## 3.10 Certificates.

Certificates are digital blobs that can be used to identify devices, owners, keys, organizations, issuers or other entities. MagTek is a Certificate Authority for its devices and users. The Certificates may include an expiration date. They are also revocable in the event of misuse.

## 3.11 Obfuscation.

Obfuscation is another useful tool. While not as powerful as encryption, obfuscation allows us to hide data in plain site. It’s like hiding a tree in a forest. With digital obfuscation, we can propagate the digital forest with zeros and ones, to protect a set of sensitive zeros and ones. And because it is a digital forest, we can move the sensitive material and re-propagate the digital forest with every use or at certain intervals.

## 3.12 Masking.

Nearly every MagTek Device is capable of masking sensitive data. Masking makes the data not viewable. Primary Account Numbers (PANs) are often "masked" by blanking a section of it out or substituting other characters in its place. The masked PANs can travel through the merchants network, and then be unmasked and validated when they reach a secure data center.

## 3.13 Noise Analysis.

Like obfuscation, noise can be used to protect sensitive data. There are many sources of noise that can be injected into a message. When the message arrives at a secure data center, the noise can be removed. Imagine a very noisy bar, with hundreds of people talking loudly. Your message is lost in the din, and you cannot shout loudly enough to overcome the noise. But if the noise can be filtered out, your message can be understood.

## 3.14 Whitelisting.

Whitelists for IP addresses, certificates or device profiles are an easy way to limit who can talk to you. For example, with an IP whitelist, if your IP address is not on the list, you will receive a standard message – Access Denied.

## 3.15 Coordinates and Pointers.

When the field of authentication data is large enough, we have the luxury of selecting the data from different sections of the digital space. Much like the way we use longitude and latitude to return to a known point on a map, in an authentication scheme an extra layer of protection is introduced when the adversary does not know where to look for the data, because he does not know the geo-coordinates or the starting point, which vary per use. We use an index to locate or relocate the authentication data, by using another field which is known to be unique to the user, device or object.

## 4 Contact

Please talk to us about your transaction security needs. With our Hardware, Firmware, Software, Cardware, Gateway and Security services, we are certain to have a bundle that will meet your needs. Call 800-MAGTEK1 and schedule a meeting.

## 5 About MagTek

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. For more information, please visit www.magtek.com.