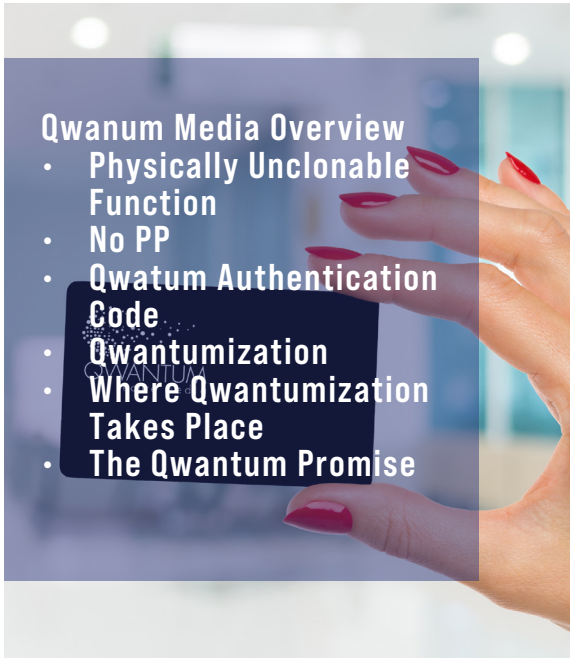
QWANTUM

Qwantum Media

Authentication Codes - White Paper

Qwantum Media is a division of MagTek that supplies Cards or Tokens, in various shapes and materials. The devices cannot be cloned or altered, do not contain a PAN or sensitive data, and provide Qwantum Authentication Codes.



Physically Unclonable Functions

Qwantum cards are endowed with a Unique Magnetic Particle Pattern which serves as a digital fingerprint. Every high-coercivity magnetic stripe card carries a Physically Unclonable Function or a PUF. In the world of Quantum Physics, a PUF is a physical entity, embodied in a physical structure that is easy to evaluate but hard to predict. One major way that PUFs are categorized is based on examining the source of the randomness or variation, from which the PUF is derived. This source of uniqueness is either applied in an explicit manner, through the deliberate addition of extra manufacturing steps (like a coating), or occurs in an implicit manner, as part of the typical manufacturing processes.

All PUFs depend on the uniqueness of their physical micro-structure. This micro-structure depends on random physical factors introduced during manufacturing. These factors must be unpredictable and uncontrollable, such that it makes it virtually impossible to duplicate or clone the structure.

A magnetic PUF is based on unique physical variations which occur naturally during manufacturing. The physical structure of the magnetic stripe applied to a card is fabricated by blending billions of particles of barium ferrite together in a slurry during the manufacturing process. The particles have many different shapes and sizes. The slurry is applied to a receptor layer. The particle distribution is random, much like pouring a handful of wet magnetic sand onto a carrier. To pour the sand to land in exactly the same pattern a second time is physically impossible due to the inexactness of the process, the sheer number of particles, and the random geometry of their shape and size. When the slurry dries, the receptor layer is sliced into strips and applied to plastic cards, but the random pattern on the magnetic media remains. This randomness introduced during the manufacturing process cannot be controlled or predicted or duplicated, but the PUF can be read. This magnetic PUF is a classic example of a PUF using implicit randomness. It is this property which assures that a Qwantum card cannot be counterfeited or altered without detection.

No Personally Identifiable Information (PII)

Qwantum Cards or Tokens do not carry or emit machine-readable Primary Account Numbers (PANs) or Personally Identifiable Information (PII). PANs and PII are hazardous data. Qwantum cards have an optional number which identifies the card, but does not provide any information related to the cardholder. In a pure Qwantum Card world, there are no Names, no Account Numbers, or anything that will betray consumer personal data. If numbers and data exist on the card or token, it is merely to identify the device itself. The encoded data identifies the token, the Qwantum data authenticates the token, and possession of the unique token establishes ownership and authenticates the User.

Qwantum Authentication Codes (QAC)

Qwantum Authentication Codes are based on the principles of Quantum Physics. They morph with every use. Literally, just touch the card and its Qwantum output will change.

Qwantum Authentication Codes (QAC) are:

- Dynamic Digital Codes emitted by the Card
- Derived from an underlying Magnetic PUF

As in Quantum Mechanics the Codes are

- Unpredictable
- Non-repeatable
- Un-alterable
- Used only once
- Verifiable by Quantum Correlation to the root QAC – proven provenance

Qwantum Authentication Codes can be used like a key to grant permission to:

- Download software
- Log-in
- Access a building
- Retrieve an API
- Update a configuration
- Open a door
- Authorize a financial transaction
- Attest to an approved transaction
- Inject a key
- Install a certificate
- Redeem points at POS
- Obtain Rewards or Coupons
- Any other use where “UserName and Password” is insufficient. (There are too many to list)

Codes can be delivered directly from the card swipe or delivered to a phone, tablet or PC from Magensa HSMs.

Shortened QAC: Qwick Codes

Qwick Codes are a shortened version of a Qwantum Code. Easy for a consumer to remember or enter, Qwick Codes are an index or pointer to a valid Qwantum Code.

Qwantumization

Qwantumization is an enrollment process whereby:
1) the encoded data is frozen - Read only Technology
2) the Dynamic Data is enabled - Touch me - I change
3) the Root Qwantum Authentication Code (an intermingling of the frozen data and the dynamic Data) - RQAC is recorded

Where Qwantumization takes place

The best place to capture the Root Qwantum Authentication Code is during manufacture or personalization. Here, the Qwantum value is authoritative because it was captured in a controlled card issuing process. It’s also possible to capture Qwantum Codes in the wild.

A Quantum equipped reader can pick up the Qwantum Code, mark it as provisional, and send it to storage for future use. When the pedigree of the code is undisputed, the Qwantum Code can be elevated to the Root QAC.

The Qwantum Promise

If the card:
1. bears a Qwantum Logo
2. and has been registered by Magensa or MagTek
3. and receives a passing score in the Qwantum Authentication Engine
4. and is actually counterfeit or the relying data has been altered

MagTek will absorb the financial loss due to the fraudulent transaction*.

* Limits, terms, and conditions apply.