QWANTUM
A MAGTEK PLATFORM

Qwantum™ Tokens and Qwantum Multi-factor Authentication (QMFA): The Powerful Claims Architecture

MagTek's Qwantum Platform is a next-generation tokenization and authentication framework designed to replace outdated security models with real-time, user-initiated, and cryptographically secure authentication of Qwantum Tokens. Qwantum Tokens can be used in place of legacy credentials and used for specific purposes, such as granting access to a facility, to a cash drawer, to a website, to loyalty points, even to stored value for tickets, coupons and closed loop payments.

The platform supports physical Qwantum Cards, NFC wearables, barcodes and other digital data, offering a mobile-first, yet flexible approach to eliminate static credentials that contain personally identifiable information (PII), prevent fraud, while strengthening and modernizing access and identity management.

The Qwantum Platform is based on an extensive set of APIs, embedded circuits, hardware and services that have been integrated to generate powerful tokens including custom branding, advanced delivery options, lifecycle management, and redemption services, all backed by powerful Qwantum Multi-Factor Authentication or QMFA.

Qwantum Tokens and Claims

Qwantum's advanced architecture is based on three sources of claims, enabling **Contextual Authorization** where the access decision can be made from any permutation of these attributes:

1. User's Claims (The Who): This is the persistent dictionary of a user's identity attributes, stored securely on the QMFA backend service. This profile provides the baseline identity, and required metadata, with minimum keys including **Username**, **Firstname**, **Lastname**, **Email**, and **SMSNumber**. Beyond these basics, this dictionary can include claims with organizational attributes such as **{loyalty_tier: Gold}** or **{department: Finance}**. These claims are essential for linking the user to their tokens and defining their standing privileges. This layer can also store or reference a globally specific **OTC**, **TAC**, or **TOTP** associated with the User's profile for general user-level authentication.

2. The Token's Claims dictionary (The Temporary What, When, and How): This is the dynamic set of authorization rules associated with the unique cryptographic token identifier on the QMFA backend. **Crucially, the token itself is a secure, non-descriptive key; it contains no PII or clear text claims.** These Claims define the short-lived constraints and specific values for the transaction or access event. Examples of these rich data points include **Account Data and Balances**, **Seat #s**, a **Status label** (e.g., VIP), and a specific **Day and time of access** (exp). The Claims can also require augmented authentication factors, such as a limited-life **One Time Code (OTC)**, a persistent **Timed Access Code (TAC)** value, or a continuously regenerating **Time-based One-Time Password (TOTP)**. This layer allows for **transaction-specific authentication** where the factor secures a specific asset or action, providing security that is unique to the token itself.

3. Device's Claims (The Contextual Where): This dictionary contains validated, session-specific data transmitted by the secure reader or application, including the device's unique ID (device_id), validated geographical coordinates (geo_location), and the scan timestamp. These claims are vital for implementing risk-based policies that enhance the security of the overall authorization scheme.

Use Case Applications and Architectural Benefits

Qwantum's strength lies in its ability to adapt its claims architecture to diverse real-world needs, leveraging the **Permutation-Based Authorization** model across all three claim dictionaries:

Point of Sale and Merchant Services

- **Opening a Cash Drawer or Safe (Dynamic OTC):** In high-stakes retail or banking environments, opening a cash drawer requires immediate, non-repudiable authorization. The Token's Claims define the specific `Hardware_ID` and `Access_Level`. When a cashier or manager scans their Qwantum Token, the QMFA system generates a dynamic One-Time Code (OTC) that is valid only for that specific terminal at that exact micro-second. This eliminates "buddy-swiping" and ensures every drawer opening is logged against a unique, non-reusable event.
- **Manager Batch Closing (Role-Based Claim Validation):** Closing a financial batch requires elevated authority. Here, the process depends on the User's Claims (Role: Manager). When the manager initiates the close, the system checks the token against the backend to verify the manager's current employment status and

authorization level. If the manager was terminated ten minutes prior, the token is revoked in real-time, preventing unauthorized financial settlement.

- **Car Wash Closed-Loop Payments, Coupons, and Loyalty:** In this example, the car wash relies on the **Token's Claims** to manage transactional value. A single token can manage a customer's loadable **Balance** (for payment), store a single-use **Coupon: Premium_Wash** (conditional access), and track **Loyalty_Credits**. The backend securely updates these claims after every scan and transaction, consolidating complex commerce and reward logic into one system.
- **The Tokenized Concert Ticket and Transfer:** The ticket's authority, defined by its **Token's Claims** (e.g., **seat_section: Floor B**), is independent of the owner's identity. When the token is transferred, the **Token's Claims** remain valid, but the access privilege is always evaluated against the current owner's **User's Claims** (e.g., Bronze loyalty tier), accurately reflecting the new owner's access.
- **Time & Attendance (Geofenced Tokens):** To prevent "proxy punching," Time & Attendance tokens leverage claims that can include `Location_Boundaries`. The token is only valid when the User's Claims (GPS location from the QMFA Wallet) match the Token's Claims (the job site coordinates). This ensures employees are physically present when clocking in, providing an unforgeable audit trail for payroll.

Financial and Banking Services

- **High-Value Withdrawals (Multi-Dictionary Validation):** For withdrawals from fixed accounts, the system evaluates three dictionaries. The Token's Claims define the `Daily_Limit` and `Account_Type`. The User's Claims verify the `KYC_Status`. Finally, the TAC_Value (a PIN known only to the customer) acts as the third factor. This ensures that even if a physical Qwantum Token is stolen, the thief cannot withdraw funds without the out-of-band TAC.
- **Teller and Customer Transactions (Mutual Authentication):** In a banking hall, both the teller and the customer use QMFA. The customer's token provides `Account_Access_Authority`, while the teller's token provides `Transaction_Processing_Authority`. The transaction only proceeds when both sets of claims are cryptographically joined, ensuring that neither party can act unilaterally without a secure, logged interaction.

- **Safety Deposit Box Access (Dual-Token Possession):** Accessing a physical safety deposit box traditionally requires two keys. In the QMFA model, this is digitized. The vault entry requires the Token's Claims from the bank's master token and the Token's Claims from the customer's Qwantum Card. The system validates that both tokens are present and active, creating a digital "dual-shrouding" environment without the risk of lost physical keys.
- **Risk-Based Transaction Approval:** Use **Token's Claims** for the transaction details (e.g., **transaction_amount: $5000**) and require the factor to be a **Token-specific OTC** only if **Device's Claims** show the login location (geo_location) is outside the usual geographic radius for the user.
- **Secure Wire Transfer Authorization:** Require a unique, **Token-specific TOTP** to secure the transfer request. The authorization policy checks that the user's permanent **User's Claims** (role_level: Manager) and the **Token's Claims** (max_amount: $10,000) are both valid before the transfer is executed.
- **Customer Onboarding/KYC Access:** Issue a temporary token with a low **exp** claim (e.g., 24 hours) for a new customer to securely upload necessary documents, eliminating the need for a static password during the initial sensitive process.

Healthcare/Patient Data and Government

- **Medical Records Access (Contextual Privacy):** Medical privacy relies on the "Minimum Necessary" rule. The Token's Claims define the `Department_Scope` (e.g., Radiology), while the User's Claims define the `Professional_Credential` (e.g., Registered Nurse). When the nurse scans to enter a record, the QMFA system only releases the specific data fields allowed by that intersection of claims, protecting patient PII/PHI while ensuring the nurse has the information required for care.
- **Call Center:** Traditional call centers often rely on static Knowledge-Based Authentication (KBA), such as asking for a mother's maiden name or the last four digits of an SSN. This static data is frequently leaked in breaches, making it easy for bad actors to "spoof" or social-engineer their way into accounts. By integrating the **QMFA API** into the CRM or agent portal, organizations can verify a caller's identity by using secure, single-use and/or time-based limited use credentials.

- **ID Verification:** Use a non-PII token to securely link a person to their digital records. A scan of the token at a service desk requires a **Token-specific OTC** for identity proofing, ensuring that the person physically presenting the token is the authorized owner before accessing sensitive information.
- **Supply Chain/Asset Management:** Issue Tokens for high-value medical equipment. **Device's Claims** (from a scanner or application) are used to confirm the item's location (**geo_location** is within a secure warehouse) before granting a user permission to update the item's **Token's Claims** (e.g., changing its **Status label** from *in transit* to *stored*).

Identity and Restricted Access

- **Age-Restricted Access and Purchases (Anonymized Proof):** For purchasing alcohol or entering a gambling floor, the system utilizes User's Claims to provide a "Zero-Knowledge Proof." Instead of the merchant seeing the user's birthdate or address (PII), the QMFA system simply returns a `Boolean: True` for the claim `Is_Over_21`. This confirms authorization without exposing sensitive personal data to the merchant's database.
- **Contractor/Visitor Access:** Issue a token secured by a simple, persistent **TAC** for a visitor. The **Token's Claims** define the **access_points** (e.g., only lobbies and elevators) and a strict **exp** date (e.g., end of day), while **User's Claims** simply define them as **status: contractor**.
- **Secured VPN/Remote Desktop:** Implement token-based access where the **User's Claims** require the use of their **Global TOTP** factor and the authorization check verifies the **Device's Claims** (e.g., **device_id** or **os_version**) against a corporate whitelist before granting VPN access.

Membership and Hospitality

- **Family Resort Access (Persistent TAC):** This demonstrates security for shareable assets. A single token is issued for a family resort stay, secured by a persistent **TAC** (PIN). The **Token's Claims** define the token's validity, including the **exp** date for mass revocation and the **TAC_Value** for secondary authentication. The QR code can be freely shared among the family, but anyone copying it **must know the TAC** as that value would be delivered to the Token Owner through an out-of-band channel such

as email or SMS. Using that token to complete a transaction would require knowledge of the assigned TAC, providing secure, instant access while ensuring mass revocation at the pre-defined check-out time.

- **Membership Access and Loyalty (Tiered Authority):** In a private club or gym, the Token's Claims may simply grant `Gate_Access`. However, the User's Claims define the experience. A "Gold Member" claim might trigger a welcome message on a kiosk or unlock a premium locker room, whereas a "Standard Member" claim only opens the front door. The hardware remains the same; only the claims change.

Education and Campus Access

- **University Testing Admittance (Credential Integrity):** To prevent academic fraud, a student's Qwantum Token is tied to a specific `Exam_ID` and `Seat_Assignment`. Upon entering the testing center, the student scans their token. The backend verifies the User's Claims (Enrollment Status) against the Token's Claims (Test Authorization). Because the token is dynamic, it cannot be screenshotted or sent to a third party to take the test in the student's place.

- **Student ID & Campus Access:** Use the student's primary Token for physical access to dorms, libraries, or labs. The authorization policy checks **User's Claims** (e.g., **student_status: enrolled**) and **Token's Claims** (e.g., **access_points: Lab_005**), with a quick secondary factor like a persistent **TAC** for enhanced security at the dorm entrance.

- **Exam Proctoring Access:** Issue a specific, single-use **Token** for an exam secured by an **OTC**. The **Token's Claims** define the **course_id** and have **max_uses: 1**. The student must scan the QR code and enter the OTC to begin the online exam, validating that the student has paid and preventing repeat attempts.

Casinos & Gaming

- **Gambling and Gaming Access (Responsible Gaming Limits):** In a casino, a Qwantum Token can manage a player's "Session Limits." The Token's Claims store a `Loss_Limit` or `Time_Limit`. As the player scans at various machines, the claims are updated in real-time. Once the limit defined in the claims is reached, the token automatically denies further "Buy-In" authorizations, supporting responsible gaming compliance.

- **VIP Access & Entitlements:** Issue a **Token** where **Token's Claims** include **Status label: HighRoller** and **access_area: PrivateGamingSalon**. This is used at a secure reader where the authorization policy also checks the **Device's Claims** to confirm the scanner is located at the correct lounge entrance.

Human Resources (HR)

- **Employee Record Access (Digital):** Secure access to sensitive HR files via a web portal. The authorization policy requires the **User's Claims** to include **department: HR** and mandates a successful **Global TOTP** authentication, ensuring the user is verified before the system grants access to documents (Token's Claims defining the **document_category**).
- **Policy Acknowledgment:** Issue a temporary **Token** secured by a **Token-specific OTC**. The employee must use the OTC to access and digitally sign a mandatory compliance document. The **Token's Claims** are then updated with a **policy_acknowledged: True** stamp, providing a non-repudiable audit trail.

Sporting Events & Venues

- **Dynamic Season Ticket Management:** Issue a permanent season ticket Token. For each game, the **Token's Claims** are dynamically updated on the backend with the current **Game_ID** and a single **max_uses: 1**. This ensures the same physical QR code is instantly ready for the next event without needing re-issuance.
- **Venue Purchase/Concessions (Cashless):** Integrate the Token with the customer's pre-loaded account. **Token's Claims** hold the **Balance** and **VIP_discount_rate**. A simple scan at concessions instantly authenticates the customer and applies the correct discount based on the Token's Claims.
- **Team Locker Room Access:** For players and staff, restrict access using a **Token** secured by a **TOTP**. The authorization policy checks that the **User's Claims** include **role: Player_Active** AND **Device's Claims** (from the reader) show the access point is **location_ID: Home_Locker_Room**.

Administrative and System Security

- **Admin Level System Access (Ephemeral Privilege):** Granting "Root" or "Admin" access is a high risk. QMFA allows for Ephemeral Claims. An IT professional is

issued a token where the `Admin_Status` claim is only valid for a 4-hour window. Once the window expires, the token automatically reverts to a standard user level, eliminating the "permanent admin" vulnerability that hackers often exploit.

- **Transaction Signing (Cryptographic Attribution):** For legal or high-value contracts, the QMFA Wallet can provide a "Signing Signature." The Token's Claims include a hash of the document being signed. By authorizing the transaction with the Qwantum Token, the user creates a cryptographically bound link between their possession of the token and the specific version of the document, providing a higher level of non-repudiation than a standard e-signature.
- **Secure Digital Access to a Website (TOTP/OTC):** For sensitive platforms like the Magensa Merchant Portal, the **Token's Claims** define the **URL** and **Form_Fields** for automated login. The QMFA Wallet app opens the site and automatically injects the user's static data alongside a dynamic factor (TOTP or OTC) for seamless, multi-factor login, eliminating static password risk. It's important to note that in this example, the static data contains no PII.

Extensibility, Security, and Transferability

The superior design of Qwantum Tokens is defined by three key architectural elements that are strong selling features:

1. **Zero-Downtime Extensibility:** The QMFA backend leverages a **NoSQL (MongoDB-like) database model** which supports a dynamic, schema-less structure. This allows clients to instantly add custom attributes to the User's Claims dictionary without any database downtime or costly, time-consuming **schema migrations**.
2. **Secure Authorization Flow:** The MagTek Dyna Device acts as an **optional, authorized secure reader** for QMFA. While QMFA does not require a Dyna Device for all use cases (like a digital web login), adding one enhances physical security. The device's primary function is to securely read the Qwantum Token's globally unique identifier and transmit that information to the backend. **Critically, the Dyna Device does not evaluate the token or its claims.** The QMFA backend is the sole source of intelligence, performing all authentication, claims retrieval, and authorization logic against the combined claims data, which may include additional claims contributed by the Dyna Device (such as its unique ID or geo-location) to enhance the authorization scheme.

3. **Seamless Asset Transfer:** The token's authority is independent of PII. The **Token's Claims** are transferred with the asset, but the access privilege is always evaluated against the current owner's **User's Claims**.

In summary, the Qwantum Platform's architecture is built for security, agility, and performance, using dynamic, dictionaries of claims that are centrally managed and evaluated, ensuring trust that scales for a variety of markets and needs.

###