digital card issuance and emergency card replacement
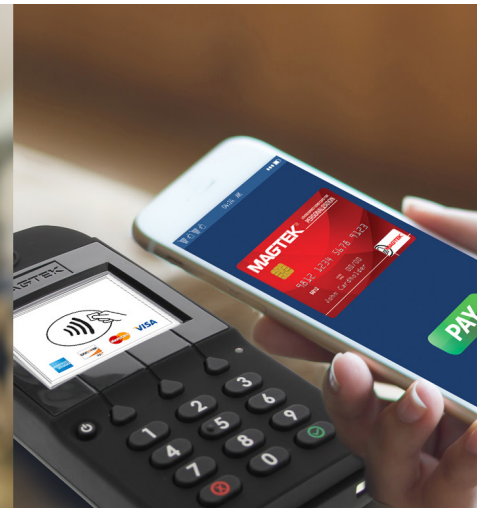
QwickCards

QwickCards is a cloud-based, digital card issuance and PIN service brought to you by MagTek. QwickCards provides an easy-to-use browser-based platform to make digital card issuance and PIN selection safe, economical, simple, and fast. Expensive and mechanically complicated card personalization machines are not needed, affording the financial institutions the opportunity to provision digital cards in real-time, while relying on in house or external service bureaus to issue physical cards when needed. As more commerce is transacted in a mobile and touchless manner, digital cards and mobile wallets are becoming even more popular. Digital card issuance with QwickCards can give you the competitive edge you need to attract and maintain deposit accounts and top of wallet consistency.

Digital Card Issuance and Emergency Card Replacement

If you need a digital card solution now, QwickCards includes a full-feature platform that securely delivers digital card information to your cardholders. By incorporating Qwantum Private Messaging with QwickCards, banks and credit unions transmit sensitive card data directly to cardholders where the data is encrypted with a unique AES-256 encryption key per transaction. Cardholders then receive a separate unlocking token, enabling 2-factor authentication with geo-location tagging to gain access to the digital card data. This process is fast, efficient, and highly secure providing the financial institution with an immediate receipt, proving delivery, and access to the digital card data by the intended, authorized party.

Benefits of Cloud-Based Software

MagTek delivers scalability via its cloud infrastructure and around the clock performance monitoring. QwickCards is a proven platform deployed to financial institutions ranging from single branch locations to hundreds of branch locations. With QwickCards, your digital card issuance and PIN transactions are secure, fast, reliable, and cost-effective. QwickCards is hosted at Magensa, MagTek's PCI Level 1 certified gateway and token exchange. QwickCards follows best practices (including meeting PCI PIN compliance) and industry leading methodologies for protecting sensitive card and personal data.

Lower cost, lower capital investment

QwickCards delivers high-end technology at a fraction of the costs associated with software-in-a-box models. QwickCards is founded on redundant safeguards and firewalls. This reduces hardware costs, hosting fees and on-going maintenance costs, allowing the savings to be passed on to you. Due to the nature of cloud-based software, project launches typically roll out faster, cost less, and have predictable operating expenses. Your institution will reap the financial benefits while helping to reduce your CO2 footprint.

Cloud Scalability

QwickCards is scalable and flexible and designed to accommodate your needs. MagTek manages the provisioning and bandwidth as needed, so you can focus on your cardholders and their needs.

Flexible Hardware and Software

QwickCards is flexible and supports deployments on desktop and tablet PCs. PIN Encrypting Devices (PEDs) are available with USB, Bluetooth LE or 802.11 wireless interfaces. Software releases and upgrades are free of charge and automatically deployed when available and come without the need to install or make changes to your back-end systems.

Ease-of-use

QwickCards is easy to use and simple to navigate. With continual customer feedback, our solution only gets better. MagTek strives to provide the best user interface, so you can provide your consumers with instant purchasing power. Now you can offer digital card issuance, emergency replacement card issuance, PIN and rePIN from on-site or off-site, at college fairs, bank conferences, and sports venues.

Application Security

QwickCards uses the MagneSafe Security Architecture to deliver the most secure multi-factor authentication sign-on experience and eliminates security concerns of static, counterfeit, altered or stolen login credentials. QwickCards delivers dynamic data with every sign-on, providing robust security and never relying on static login credentials. Unlike usernames and passwords, every QwickCards login provides one-time use data that affirms the authenticity of the user and their access privileges.

Administration

QwickCards allows you to manage your branch locations, devices, and service representatives. If service representatives need to float between locations, their rights can vary or stay the same based on the location. Reports and Administrative details are all accessed from one point, and therefore they are universal across your institution. No need to coalesce or compare reports with mixed formats. QwickCards delivers a single point of access.

Green Benefits

With QwickCards, your consumers don't have to wait to receive PIN mailers. There are no lost or stolen card mailers and no loss of transactions during the typical 7-14 days transit time realized with service bureau issued cards. Digital cards are fast, inexpensive to issue, and accepted almost everywhere. Green benefits are achieved because of a lower CO2 footprint and with no expensive and mechanically complicated card personalization machines to maintain; your financial institution saves time and money!

PIN and rePIN Programs

QwickCards is a ready to go platform that uses MagTek quality hardware and security for fast and easy PIN selection. Give your consumers the ability to personally select their own PIN and let them walk out of your branch with a fully activated digital card. Consumer-selected PINs are easily remembered, and studies have shown that they lead to increased card usage. This service enhances your brand and reduces costs associated with wait time, PIN mailers, and potential fraud losses.

Host-Based PIN Offsets

MagTek's PIN Encrypting Devices (PEDs), such as DynaPro Go, can help to securely generate encrypted PIN blocks that can be used for PIN verification at the teller window. QwickCards can also provide calculated PIN Offsets to your core or processor.

Reliable Hardware - DynaPro Go

Protect PIN data and safely login with a secure PIN Encrypting Device such as DynaPro Go. This PIN pad and Secure Card Reader Authenticator relies on the MagneSafe Security Architecture. Using MagTek devices for PIN selection and login functions secures your cardholders and your service representatives while exceeding security standards. DynaPro Go meets and exceeds PCI PTS 4.x, SRED security requirements and its enclosure and associated electronics form a Tamper Resistant Security Module.

Interface Connection: QwickInterface

QwickInterface provides a direct and secure connection to your core or processor. Most major interfaces are currently supported, and MagTek's Application Program Interfaces (APIs) simplify development. If your institution has an interface that is not currently supported, our in-house development team can make it happen.

Engineered Security

MagTek takes transaction security seriously and understands that your security systems extend beyond the transaction and into lasting relationships. You require business continuity, agility and a team working for you. As a manufacturer of card and PIN personalization systems, MagTek secures its products throughout the entire life cycle. From the factory to delivery, activation, key management, implementation, on-going use, and final disposition, your devices and systems remain secure.

Emergency Card Replacement Diagram

FINANCIAL INSTITUTION ISSUES DIGITAL CARD

FINANCIAL INSTITUTION SENDS DIGITAL CARD TOKEN TO CONSUMER

CONSUMER DECRYPTS DIGITAL CARD TOKEN

CONSUMER ADDS CARD TO MOBILE WALLET

FINANCIAL INSTITUTION RECEIVES RECEIPT

Your card has been digitally issued. You can add this information to your mobile wallet and begin to make purchases or withdraw cash anywhere mobile wallets are accepted.

Financial institution creates a one-time use and unique Qwantum Guest Token and sends it to the consumer.
QPM Guest Token: NjYyMzYzZTEt

Consumer uses the one-time-use Qwantum Guest Token issued by the financial institution to securely unlock and decrypt the digital card data.

Consumer enters data into mobile wallet.

Your card has been digitally issued. You can add this information to your mobile wallet and begin to make purchases or withdraw cash anywhere mobile wallets are accepted.

Financial institution receives an email delivery receipt and geo-location of the receiving consumer.