QkerPass

Password-less Authentication

iSign International

iSign International® is a digital security hardware and software company focusing on Biometric Signature, Threat Detection, and Prevention. After gauging the unacceptable level of risk that passwords pose to individual users, businesses, and governments alike, we present QkerPass, a milestone in password-less authentication.

'Trustless security' or 'zero-trust security' is the future of cybersecurity solutions. And with it password-less access, a type of authentication were individuals do not need to log-in with passwords. This form of authentication makes passwords obsolete. With this technology users get the option of either logging in via a magic link, fingerprint, or using code scanning technology. 'Trustless security' or 'zero-trust security' especially becomes essential for small and mid-sized businesses or enterprises that do not have high budget allocations for information security. Government organizations are at higher than normal risks as well, where employees/staff are often ill-prepared or not sufficiently trained on cybersecurity best practices to deal with a data breach.

Benefits of Password-less Authentication

Statistical data from a Verizon report proves that more than 80% of data breaches occurred because of frequently reused or weak passwords. The reason why individual users, organizations, and governments find password-less authentication useful is because it:

- **Improves User Experience:** For enterprises, the faster users can sign up and use their service, the more users the app tends to attract. Users find it

cumbersome having to fill out forms and going through a rigorous registration process. Also, it is cumbersome to remember passwords!

- Increases Security: Once users go password-less, there are no vulnerable passwords that the adversaries can target.

What Is QkerPass?

QkerPass eliminates the requirement of username and password entry for any web-based application. With a simple scan using the QkerPass app, individuals can quickly and securely sign into their applications. This module is easy to deploy for any organization via an API generator delivered and deployed upon request.

Advanced Features

QkerPass comes with state-of-the-art Dynamic PKI Encryption, Artificial Intelligence, End Point Server Security, and Actionable QR Profile Blockchain. These are just some of the 6 Factors to protect individual users, enterprises, and governments alike.

- Profile Blockchain to eliminate hacking attempts: Blockchain is a shared, immutable ledger that records transactions, tracks assets, and builds trust. Its elements are:
  - Distributed ledger technology: All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, thus eliminating the duplication of effort that is common in traditional business networks.
  - Records are immutable: No participant can change or tamper with a transaction after it is recorded in the shared ledger. If a transaction record includes an error, adding a new transaction is required to reverse the mistake, and both transactions are then visible.

- **Smart contracts:** To speed transactions, a set of rules – called a smart contract – is stored on the Blockchain and executed automatically. A smart contract can include terms for travel insurance, payment, define conditions for corporate bond transfers, and much more.

- No username and password
- Advanced Access Analytics
- Patented Dynamic PKI Encrypted End-to-End Communication: End-to-end encryption (E2EE) encrypts the user's message throughout its journey between two endpoints. It stays encrypted while traveling through intermediate servers, and neither the ISP nor any third party can access it. Without E2EE, the message is encrypted once it reaches a mid-point server that decrypts it. Thus, an entity that controls these servers (e.g., an ISP) might see the messages.
- Frictionless and Secure!
- Protection from unauthorized access.

Features	Traditional Passwords	Passwordless: QkerPass
Authentication	2 Factor	6-Factor
Risk	High	Low
Analytics	✗	Full Analytics
Ease of use	✗	✓
AI Automatization	✗	✓

Ease-of Use Packed with All-Round Protection

- **Artificial Intelligence:** Detects and acts on scanned QR. Deep-learning artificial intelligence technologies and artificial neural networks are quickly evolving. This is because AI can process large amounts of data much faster, and make predictions more accurately, than humanly possible.
- **Full Analytics:** Enterprises get full insights into their user's sign-in behaviors. User behavior analytics (UBA) is a method for collecting, combining, and analyzing qualitative and quantitative user data to track how and why users interact with a product or website.
- **Easy Data Passing:** Users can scan a QkerPass to send information from their mobile devices. Some barriers, like the need to maintain user privacy, are common to all users and organizations. With QkerPass, they can rest assured that the data passes on securely.
- **Full User Management:** QkerPass allows governments to manage their users from anywhere. User management offers a score of benefits for individual users like:
  - Improved user experience
  - Enhanced security profiles

  Apart from these, efficient user management provides benefits to, both governmental and private, organizations like:

  - Simplified auditing and reporting
  - Easy access no matter where the employees are
  - Increased productivity and reduced Information Technology (IT) costs
- **Multi-Account Support:** QkerPass supports multiple accounts with a single application. It is a boon for users who have a single device operated by various family members. They can use QkerPass to log in to their favorite applications.
- **Full API:** It is impossible to imagine modern technology without APIs. API is an interface that allows the application to interact with an external service using a simple set of commands. Users can quickly integrate QkerPass with cut and

paste API. If your organization needs an on-prem deployment, please let us know as we can accommodate.

Conclusion

There is no doubt that passwords are becoming obsolete, and more susceptible to hacking attempts in recent years. Organizations around the world are shifting to a new paradigm of 'trustless security' or 'zero-trust security,' where remembering 'usernames' and 'passwords' is becoming a thing of the past. Password-less authentication aims to eliminate authentication vulnerabilities. QkerPass, from iSign International, is a Blockchain-based solution that has embraced iSign's patented End-to-End Dynamic PKI Encrypted Communication technology with 6-Factor Authentication (6FA) and enables individual users, organizations, and governments to take their information security to the next level.

To learn more about iSign and its SmartGuard innovative solution, which helps monitor and detect malicious activities in real-time by leveraging hardware-assisted security assurance for home and business environments visit our website at https://isigninternational.com/.