

# Survey on Q5id



## Agenda

1. Top Identity Management Software
2. about Q5id
3. FAQ in Q5id
4. Features of IDaaS
5. Compliance for GDPR

# Top Identity Management Software

## Market Share

- USD 3.85B in 2020, USD14.82B by 2025, CAGR : 31.2%
- IDaaS market share(2021)
  - Okta 47.2%
  - MS 17.4%
  - Ping Identity 6.4%

## 1. Okta

- Cloud-Based
  - features : SSO<sup>1</sup>, MFA<sup>2</sup> and User provisioning
- <sup>1</sup>SSO : Single-Sign On
- <sup>2</sup>MFA : Multi-Factor Authentication

## 2. Azure Active Directory

- Cloud-Based
- features : SSO, MFA and Conditional Access Policies
- provides authentication and authorization

### 3. Ping Identity

- Cloud-Based
- features : SSO, MFA and User provisioning
- Secure access for app and APIs

### 4. ForgeRock

- Open-source
- features : SSO, MFA and User provisioning

## 5. SailPoint

- Cloud-Based
- provides visibility and control over user access to applications and data.
- features : identity governance, access certification, and user provisioning

## 6. OneLogin

- Cloud-Based
- features : SSO, MFA and User provisioning

## FAQ about Q5id

- **Store Personal and biometric data**

Data, such as name, address, email, and phone number are **encrypted and saved.**

Unless required, biometrics are not stored. Biometrics are converted into a character string using a hashing algorithm that cannot be reverse-engineered.

Images may be stored when required by law or regulations specific to a given business. Any images we do store are **secured in a data vault.**

- If an individual wants to use their Q5id Proven Identity with more than one company, do they have to prove their identity multiple times?

**No** . Proving your identity only needs to be completed **one time** .

Once proven, your identity can be used to authenticate transactions with an **unlimited number of companies** based on their identity requirement.

- **Delete my Proven Identity account?**

Q5id is **compliant with CCPA and GDPR** , meaning that any user can request their profile and associated data removed.

- **Regulatory compliances and industry standards**

Q5id is compliant with vertical industry requirements such as **KYC and AML** , as well as regulatory compliance with **CCPA, and GDPR** .

- **Only one Proven Identity with Q5id per each person**

Each person only has **one** identity, so each person only has **one** Proven Identity



- **Store Personal and biometric data**

Data, such as name, address, email, and phone number are **encrypted and saved.**

Unless required, biometrics are not stored. Biometrics are converted into a character string using a hashing algorithm that cannot be reverse-engineered.

Images may be stored when required by law or regulations specific to a given business. Any images we do store are **secured in a data vault**.

# Features of Q5id

- prevent fraud, reduce risk, and improve customer experience
- uses a combination of biometric and identity verification
- Overall features:

1. Q5id Identity Proofing  
uses government-issued IDs and biometric authentication
2. Q5id Biometric Authentication  
uses facial recognition and voice biometrics to authenticate users.
3. Q5id Risk Scoring  
uses ML algorithms to analyze user behavior and assign risk scores.
4. Q5id Identity as a Service  
A cloud-based identity verification solution

# Q5id IDaaS

- Key features

- (1) Identity Verification  
data sources : government-issued IDs, biometric data, and public records.
- (2) Compliance  
GDPR and HIPAA. It also meets SOC 2 and ISO 27001 standards.
- (3) Integration  
integrated with existing workflows and systems  
incorporate into your identity management strategy  
supports API and webhooks.
- (4) Customization  
flexible and customizable  
offers configuration options – custom workflows, branding, and messaging.
- (5) Analytics  
real-time analytics and reporting to track key metrics  
verification success rates, user engagement, and risk scores.
- (6) Scalability  
scalable – handle large volumes of identity verifications.
- (7) User Experience  
user-friendly experience for customers and employees.  
offers a range of verification methods, mobile and web-based options.

# GDPR compliance for Q5id

- Key ways

- (1) Lawful Basis  
relies on user consent or contractual obligation for processing personal data.
- (2) Data Minimization  
only collects and processes the data that is necessary for the purpose of identity verification.
- (3) Transparency  
transparent about its data processing activities  
providing users with clear and concise information – collected, used, shared with.
- (4) Security  
industry-standard encryption  
secure storage practices to protect user data.
- (5) Data Subject Rights  
providing users with access to their personal data  
the right to have their data corrected or erased  
the right to object to the processing of their data.
- (6) Data Protection Officer  
appointed a Data Protection Officer (DPO)  
act as a point of contact for data subjects and supervisory authorities.

# Characteristics of Q5id

- Device Agnostic / Out of Band Authentication
- Simple, Remote Enrollment

An easy 4 step process guided by in-app instructions that takes less than 3 minutes.

1. Face Scan
2. Right and Left Palm Scans
3. ID Verification
4. Video Verification

- Multi-Factor Authentication

Authentication takes less than 2 seconds.

2. in-app push notification to authenticate.
3. takes a selfie and a picture of one palm.
4. The Q5id platform verifies the information
5. sends an “approved / not approved” notification back

# Data Security

- Encrypted Storage

Any data in our **databases is encrypted**, ensuring that it can't be stolen or misused. Even if it was, the encryption is such that no usable data can be recovered.

- Simplified Identity management

A single, proven identity you can use for transactions **across multiple industries and businesses**. Enroll once and use anywhere Q5id is accepted.

- Security

All data, stored and in transmission, is encrypted. In addition, Q5id converts biometric data into a **template using a hashing algorithm**. Even if a fraudster were able to get the template, it is impossible to reverse engineer the data.

# Security

- Encrypted Database
- Personal Data Storage for Data Control
  - save : Q5id
  - delete : request email to Q5id
  - move : Not available. Only Q5id

# User Experience and Convenience

- SSO over muti-Biz

# Innovation and more

- SSI, ZKP