Product Features

Compare ID photo to face scan to calculate match score

User images are never stored and biometric vectors are salted & encrypted for security and privacy

Add liveness to face verification for added security

3D face vector created for ongoing user authentication

truuth
FaceKey

Verification recorded on immutable ledger for transparency
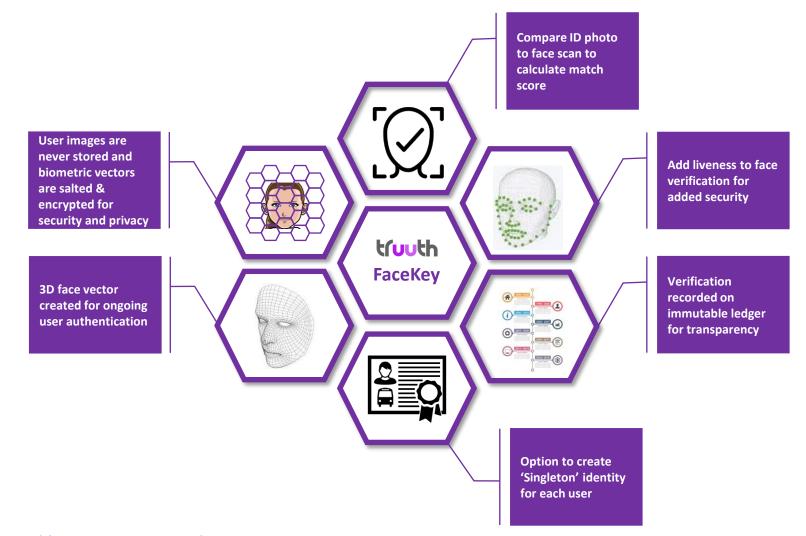
Option to create 'Singleton' identity for each user

For more details visit: https://www.truuth.id/truuth-facekey

What is truuth FaceKey?

Truuth FaceKey is a service that compares multiple face images and returns a confidence score that they belong to the same person.

FaceKey is a critical feature for verifying the identity of a user during the onboarding process. Performing a rigorous face match can mitigate the risk of identity fraud where users borrow, manipulate, or create new fake identity documents in an attempt to gain access to a service. FaceKey can also be used to replace insecure passwords an enable more secure and user friendly authentication for online services.

How does truuth FaceKey work?

Truuth FaceKey has 4 steps:

1. User scans a photo ID document and truuth FaceKey extracts the photo from the document
2. User takes a 'selfie' on their mobile device – this may include a test of liveness depending on the needs of the service provider
3. Truuth uses AI/ML models to compare the photo ID image with the selfie image and returns a confidence score that they belong to the same person
4. User chooses FaceKey to replace insecure passwords to authenticate for online services

What are the benefits of truuth FaceKey?

1. Improved security

Truuth FaceKey captures face landmark ratios from multiple images of a user during the selfie step to create a 3D model represented by X, Y, Z coordinates.

To deliver the highest level of privacy and security Truuth will never store the photo image of the user. The X, Y, Z coordinates of the 3D model are salted (false coordinates are added) and encrypted so that fraudulent actors cannot get access to the underlying biometric. For ultimate security the salted and encrypted data is sharded to different trusted servers.

Many onboarding processes still require the user to physically visit a notary with their identity documents and the notary is responsible for verifying a match between the photo ID and the applicant. A range of studies have shown this is a flawed process as many humans cannot effectively compare images. AI/ML models deliver far higher accuracy in matching faces.

For user authentication, the security risks of passwords are well documented. Replacing passwords with truuth FaceKey not only overcomes these security limitations but also delivers a substantially improved user experience.

2. Enhanced user experience

Truuth FaceKey happens seamlessly for the user. During the initial enrolment the user scans their photo ID document and then they take a selfie. This process takes less than 1 minute.

Physical (human-based) verification processes typically require multiple hours for the user to find a notary, travel to and from the notary office, and potentially repeat visits if the complete set of required documents are not furnished.

3. Reduction in Total Cost of Ownership (TCO)

Truuth FaceKey reduces the cost of onboarding a customer by enabling fully digital onboarding while mitigating risk of identity fraud.

FaceKey can be added as a feature to existing onboarding processes from less than AUD$0.10 per match.

What cyber attacks does truuth FaceKey help prevent?

Truuth FaceKey helps prevent attacks that attempt to open new accounts with fraudulent identity credentials. These include:
- Synthetic identity creation
- Identity document sharing
- Identity document manipulation
- Brute force password attack