SEVENTH SENSE

SenseCrypt

Privacy by Design

SeventhSense.AI

Content

The rapid digitization of services has transformed interactions between individuals, organizations, and governments. While online transactions offer convenience, they also expose sensitive information to cybersecurity threats such as data breaches, identity theft, and fraud. This document explores the limitations of traditional authentication methods and introduces **SenseCrypt**, an innovative solution that enhances digital identity verification through advanced cryptographic techniques and biometric authentication.

The Digital Identity Challenge

Growing Threats Outpace Traditional Authentication Methods

Traditional authentication methods, primarily relying on passwords and tokens, are increasingly vulnerable to sophisticated cyber threats like phishing, social engineering, and brute-force attacks. Passwords are often weak due to user negligence, and tokens can be lost or stolen, making these methods insufficient for current security demands.

Conventional Biometric Systems Store Biometric Data

Biometric authentication leverages unique physiological characteristics such as fingerprints and facial features for identification. While offering enhanced security, traditional biometric systems require storing sensitive biometric data, raising significant privacy concerns. Data breaches involving biometric information are particularly damaging since biometric traits cannot be changed like passwords.

Quantum Algorithms Break Widely Used Cryptographic Methods

Quantum computing poses a significant threat to existing cryptographic systems like RSA and ECC. Quantum algorithms could potentially break these widely used methods, compromising the security of encrypted data and communications. This necessitates a transition to quantum-resistant cryptographic algorithms to ensure long-term data protection.

Introducing SenseCrypt

In today's increasingly digital world, the need for secure and privacy-preserving identity verification is more critical than ever. Cybersecurity threats are constantly evolving, and the rise of quantum computing introduces new challenges to traditional cryptographic systems.

Seventh Sense addresses these multifaceted issues by combining biometric authentication with advanced cryptographic techniques, including post-quantum cryptography through its patent-pending SenseCrypt technology solution (SenseCrypt).

By introducing a novel **Face-based Public Key Infrastructure (PKI)** and **Electronic Identity (eID)** system, SenseCrypt enhances security while preserving user privacy, as it eliminates the need to store biometric data.

SenseCrypt's innovative and **first-of-its-kind** approach to biometric authentication through two different cryptographic mechanisms guarantees user privacy and GDPR compliance through its core technologies.

Integrating Post-Quantum Cryptography (PQC) with trusted SSL technology, SenseCrypt meets the growing demand for robust identity verification. This innovative approach redefines digital identity verification, making online interactions more secure, private, and future proof.

SenseCrypt also addresses the pressing issue of how to integrate biometric verification into blockchain applications and solves the problem of trusting the wallet.

SenseCrypt Technology Offerings

SenseCrypt is a suite of comprehensive solutions designed to revolutionize identity verification and secure digital interactions. It comprises four key components:

SenseCrypt eID & SensePrints

At the heart of the platform is the innovative SenseCrypt eID, which generates SensePrints – encrypted, compact data structures that serve as Verifiable Credentials. These SensePrints contain no biometric data but can be verified using the eID holder's face. Their small size (~ 350 bytes) allows for easy storage and transmission, enabling storage in NFC chips, databases or representation as QR codes.

Face-Based Public Key Infrastructure

SenseCrypt introduces the world's first Face-based Public Key Infrastructure (Face PKI). This system enables the creation of Face Certificates, which are Verifiable Presentations – standard X.509v3 certificates with public keys derived from the user's face. These certificates allow for secure transactions without the verifier ever seeing or processing the eID holder's face. The integration of post-quantum cryptography further enhances the security of Face Certificates.

Distributed Ledger Technology Protocol

This innovative protocol brings biometric verification to Distributed Ledger Technology (DLT) without storing or transferring biometric data. It solves the challenge of trusting digital wallets in blockchain applications by using a Trusted Witness system and Witnessed Credentials.

Face-Based mTLS Protocol

Currently under development, the Face-Based mutual Transport Layer Security (mTLS) Protocol aims to secure internet connections at the transport layer using face-based authentication. This innovation has the potential to eliminate the need for traditional authentication methods like usernames, passwords, and One-Time Passwords (OTPs).

SenseCrypt eID

Privacy is a fundamental right. SenseCrypt's revolutionary technological breakthrough enables privacy-focused facial verification without storing any biometric data or facial images anywhere. This GDPR-compliant technology puts users in control of their identity and data, eliminating privacy risks and ensuring complete security.

Compact Data Structure

SenseCrypt's eID solution generates **SensePrints**, which are encrypted, privacy-preserving binary data structures that serve as Verifiable Credentials. These SensePrints contain no biometric data but are biometrically verifiable using only the eID holder's live face. They are approximately five times smaller than traditional biometric templates and can be stored as QR codes, in NFC chips, or in databases.

Zero Biometric Data Storage and Privacy Preservation

Unlike traditional biometric systems that store facial images or templates, SensePrints contain no biometric data. Instead, they function as *"Locked Safes"* that can only be unlocked using the live face of the user, aligning with GDPR's data minimization principle as no biometric data is stored or processed beyond the authentication event.

Cryptographic Approach and Zero-Knowledge Face Proofs

Zero-Knowledge Face Proofs, a key feature of SenseCrypt eID, allows for face verification without revealing or storing actual facial data. This transforms face recognition from a machine learning problem into a cryptographic one, creating tokenized biometrics. Through zero-knowledge proofs, verifiers can authenticate users without ever accessing or processing their biometric data, fully complying with GDPR's data protection by design and default.

How SensePrint Works

The SenseCrypt eID system uses the user's face as the primary input, optionally combined with metadata and/or a password. A cryptographic AI algorithm generates a random ephemeral public key from the user's face, which is then used to encrypt metadata, producing encrypted bytes called SensePrints. These SensePrints, which typically contain minimal encrypted metadata and are about 350 bytes in size, can be easily converted into QR codes for various identification mediums.

- To enroll a person in traditional facial recognition systems, a template of their face is generated and stored. This template, while unique, is not privacy-preserving as it can be reverse-engineered to reveal the person's identity compared and linked across databases. In contrast, SenseCrypt eID does not store any biometrics or identity-revealing information during enrollment.
- Instead of comparing facial templates, SenseCrypt eID verification involves decrypting a given SensePrint using the correct corresponding private key generated up on a live face scan. A successful decryption verifies the person, while failure indicates a mismatch.

Unlinkability

SensePrints are inherently unlinkable, making it impossible to determine if two SensePrints belong to the same individual. This feature prevents cross-database tracking and profiling, preserving user privacy across different systems and services.

Revocability and Renewability

SensePrints can be revoked and regenerated multiple times using the same registration photo. This capability allows users to reset or update their credentials without changing their biometric data, providing enhanced security and flexibility in identity management.

Offline and Distributed Verification

SenseCrypt eID can function as a self-sovereign identity solution, allowing individuals to carry their identity in a compact form like a **QR code** ensuring every individual receives a distinct QR code linked to their encrypted identity attributes. The system's revocability feature allows users to generate new SensePrints and corresponding QR codes, enhancing security by rendering previous ones obsolete. Additionally, with a simple scan of the QR Code, SensePrints enables offline, distributed face verification without requiring communication between the issuer and verifier.

Group Verification

Additionally, a single SensePrint can be designed to verify multiple users, offering flexibility in identity management scenarios where group access or shared credentials are necessary. This feature enables organizations to manage group identities securely without compromising individual privacy.

SensePrint eIDs Are Verifiable Credentials

Multiple unique SensePrint eIDs can be issued to a single eID holder, and they are digitally signed using the issuer's private key, ensuring authenticity. Unlike standard Verifiable Credentials, SensePrint eID holder attributes are secured by requiring a face scan for decryption, adding an extra layer of protection.

Non-Repudiation

Each SensePrint is signed by the issuer, allowing verification via the issuer's root certificate public key. This ensures the authenticity and integrity of the issued electronic identity (eID), providing non-repudiation in digital transactions.

Non-Transferability

The face-based authentication ensures that only the legitimate user can use their SensePrint, preventing credential sharing or theft.

Self-Sovereign Identity

SenseCrypt eID aligns with the principles of self-sovereign identity (SSI), where individuals have control over their own digital identities.

- *User Control*: Individuals manage their SensePrints and decide when and with whom to share their credentials.
- *Privacy Preservation*: Enhances privacy by ensuring that only necessary information is shared.

SenseCrypt eID Privacy ~~Concerns~~

Storing biometric data poses significant privacy risks. If biometric databases are breached, the compromised data cannot be changed like a password, leading to permanent security issues for affected individuals. For instance, a breached biometric database allows linking an individual across different systems.

SenseCrypt eID eliminates the need to store any biometric data, addressing privacy concerns directly. By transforming biometric authentication into a cryptographic process, it ensures:

- **Data Minimization**: Only essential data is used for authentication, and none is retained after the process.
- **Reduced Attack Surface**: With no biometric data stored, there is no centralized repository for attackers to target.
- **Enhanced User Trust**: Users can be confident that their sensitive biometric information is not at risk.
- **Compliance Simplification**: By eliminating the need to store biometric data, SenseCrypt simplifies compliance with data protection regulations like GDPR and CCPA. Organizations can adopt SenseCrypt eID without the extensive regulatory burdens associated with handling sensitive personal information. Even if the issuer and verifier encryption keys are compromised, there is zero access to personally identifiable information (PII).

SenseCrypt eID Use Cases

Example 1: Secure Access Control in Corporate Environments

Companies can use SenseCrypt eID to manage user access to facilities and sensitive areas. Employees are issued SensePrints encoded in their ID badges or mobile devices. When accessing secure locations, employees scan their SensePrint and perform a live face verification, granting them access without the need for keys or cards that can be lost or stolen. This ensures that only authorized personnel can enter restricted areas, enhances security protocols, and simplifies access management.

Example 2: Offline National IDs and Licenses with SensePrints

Governments IDs and licenses with QR codes can revolutionize offline verification. Citizens receive their IDs as QR codes containing their encrypted identity attributes. When verification is needed, individuals perform a live face scan to decrypt and prove they are the legitimate owner. Authorities can verify identities offline, enhancing security as the AI capabilities greatly exceed human accuracy and consistency in verifying that a person is the legitimate ID card holder. This prevents identity fraud and unauthorized use, as only the legitimate holder can unlock the encrypted data with their live face. It streamlines services like voting, driving license checks, or accessing government facilities while complying with data protection regulations.

Example 3: Remote Education and Examination Authentication

Educational institutions can leverage SenseCrypt eID to authenticate students during class attendance and examinations. Students can use their SensePrints verifying their identity with a live face scan. This ensures that the registered student is the one attending the class or taking the exam, maintaining academic integrity without compromising student privacy. With SenseCrypt, institutions can easily comply with privacy regulations while preventing cheating and impersonation.

Example 4: Patient Identification in Healthcare Systems

Healthcare facilities can utilize SenseCrypt eID to accurately identify patients, ensuring they receive the correct treatments and medications. Patients are issued SensePrints that link to their medical records. During check-in or before procedures, patients perform a live face verification to access their records. This reduces medical errors caused by misidentification and enhances patient safety. The system maintains patient privacy, complying with healthcare privacy laws like HIPAA.

Example 5: Voting in Elections

SenseCrypt eID can facilitate secure and private voting. Voters can have voter IDs or national IDs with SensePrints. On election day, voters can authenticate themselves using a live face scan without revealing personal data. This ensures that only eligible voters can cast their ballots, reduces instances of fraud, and accelerates the voting process. The system preserves voter anonymity and integrity thereby enhancing trust in the electoral process.

Example 6: Events Ticketing

Event organizers can incorporate SenseCrypt eID for secure and efficient ticketing. Attendees receive their tickets as SensePrints on mobile devices or printed QR codes. At the event, a live face scan verifies their identity, ensuring only legitimate ticket holders gain entry. This prevents ticket fraud and unauthorized resale, enhances privacy, and streamlines the entry process, all while complying with data protection regulations.

Example 7: Hotel Check-In and Room Access

Hotels can utilize SenseCrypt eID to streamline guest check-in and room access. Guests generate their SensePrints during online booking or via hotel app. Upon arrival, a live face scan verifies their identity, and they can proceed directly to their rooms without waiting at the front desk. Check-in in remote location can be enabled by the offline verification capabilities of SenseCrypt and the storage of time-bounded access information directly in the SensePrint.

Example 8: Streamlined Airport Security and Boarding

SenseCrypt eID can revolutionize airport security by enabling passengers to verify their identity quickly and securely without presenting physical documents. Upon check-in, a passenger's SensePrint is scanned from their mobile device or a printed QR code. Security personnel verify the SensePrint using the passenger's live face. This accelerates the security screening process, reduces queues, and enhances privacy. Additionally, since no biometric data is stored or transmitted, it mitigates the risk of data breaches that could compromise passengers' sensitive information.

SenseCrypt Face PKI

While SensePrint eID requires the user's live face for each transaction, with authentication through the decryption of the SensePrint, SenseCrypt's Face PKI utilizes the construct of the well-established and accepted PKI framework and employs a unique and proprietary approach of face-derived cryptographic key pairs. Face PKI enables secure verification and transaction signing without needing the verifier to ever see the user's face – a breakthrough that sets it apart.

This world-first Face-based Public Key Infrastructure allows the creation of Face Certificates, which are Verifiable Presentations.

Face Certificates are standard X.509v3 certificates, but instead of certifying websites, Face Certificates certify individuals and enable transactions using their face without requiring access to or processing of any facial or biometric data.

Purpose-Specific Certificates

Face Certificates are generated using a combination of the user's face, their SensePrint eID, and a specific Purpose ID. The Purpose ID ensures that each certificate is unique to a particular service or function, preventing linkability across different systems and enhancing privacy protection. As in traditional PKI, the face-derived public key is embedded in a digital certificate, which can be used for authentication, encryption, and secure signing. The PKI trust hierarchy and certificate authorities are used to establish trust within the system, just as in a traditional PKI system.

Face-Derived Public Keys and Simplified Key Management

During authentication, Face PKI, with a quick face scan generates the private key on the fly, eliminating the need for expensive hardware, reducing breach risks, and easing compliance challenges. With no keys stored, the risk of data breaches is minimized, simplifying security management.

Integration of Post-Quantum Cryptography

The integration of post-quantum cryptography further enhances the security of Face Certificates. By implementing CRYSTALS-KYBER for key encapsulation and CRYSTALS-DILITHIUM for digital signatures, Face PKI ensures that Face Certificates remain secure even in the face of potential threats from quantum computing.

How Face PKI Works

At the core of Face PKI are Face Certificates, which function as Verifiable Presentations. These certificates are standard X.509v3 certificates, like those used in SSL technology to secure internet traffic, but with a crucial difference – the public key contained in the certificate is derived from the user's face. This integration of biometrics with cryptography creates a unique, privacy-preserving method of identity verification.

A Face Certificate allows a third party, without access to an individual's face or biometric data, to:

1. Encrypt information that only that person can access after a face scan, and
2. Verify that the individual signed specific information.

SSL Integration

By integrating SenseCrypt with Secure Sockets Layer (SSL) technology, the system enhances online security through robust protection. It aligns with X.509 standards, ensuring compatibility with existing PKI systems. SSL encrypts data transmission while Face PKI secures authentication, establishing mutual authentication and reducing the risk. Implementation of post-quantum algorithms ensures that data and communications remain secure as technology advances and aligns with international efforts to adopt quantum-resistant cryptography. This integration is transparent to users, maintaining a seamless user experience.

Unique Public Key

Certificates are generated for specific services or transactions using a Purpose ID, limiting their use to designated contexts and reducing the risk of misuse. Each Certificate contains a unique public key derived from the user's face. Certificates include expiry dates and a certificate revocation list URL to ensure they remain current and support immediate revocation if compromised.

Non-Repudiation and Non-Transferability

The Certificates are signed by a trusted Certificate Authority (CA), similar to traditional SSL Certificates ensuring authenticity and providing non-repudiation and that only the legitimate user can use their Face Certificate, preventing credential sharing or theft.

Encrypted Attributes

Sensitive information within Face Certificates is encrypted using a user-verifier specific public key, ensuring that only intended parties can access the data, even if intercepted. This protects data confidentiality and prevents unauthorized access.

Advantages Over Traditional PKI

Beyond its robust security features, SenseCrypt Face PKI offers significant benefits over traditional Public Key Infrastructure systems. Namely:

Reduced Risk of Key Loss

One of the primary benefits is enhanced security through simplified key management. Users no longer need to manage or protect physical private keys; instead, keys are generated from the user's face as needed. This reduces the complexity of key distribution and storage, eliminating the risk of key loss since no physical tokens or devices can be misplaced or stolen.

Zero-Knowledge Proofs

The authentication process is quick and intuitive, enhancing user experience. Users authenticate themselves with a live face scan, to generate the private key to compete transactions. Through the PKI framework, the verifier can be confident that the same face that generated the Face Certificate is conducting the transaction – without ever accessing the user's face directly. This approach prevents unauthorized use, credential sharing, and spoofing, while preserving privacy.

Enhanced Security

This approach minimizes the handling of sensitive information, strengthening overall security. By integrating strong security with ease of use, Face PKI provides a more secure, privacy-preserving, and user-friendly alternative to traditional biometric and multi-factor authentication (MFA) systems.

Face Certificates also help organizations comply with regulations like GDPR, supporting data protection by design and default, aligned with international privacy standards.

By combining these features, SenseCrypt's Face PKI offers a more secure, privacy-preserving, and legally robust authentication method. It addresses identity theft and non-repudiation in digital transactions, making it ideal for high-security applications in finance, healthcare, and government services.

Face PKI Use Cases

Example 1: Multi-Factor Authentication (MFA) for Enhanced Security

Organizations can implement Face PKI as an additional factor in their MFA systems. When logging in, users sign a challenge presented to them by performing a live face scan to generate the private key needed for authentication. This ensures that even when passwords and devices are compromised, unauthorized access is prevented, as only the legitimate user can produce the correct face-derived key to sign the challenge, which is verified in the backend using the public key inside the Face Certificate. The system enhances security, aligning with privacy regulations and improving overall organizational cybersecurity.

Example 2: Proof of Humanness in Online Interactions

Online platforms can utilize Face PKI to verify that users are real humans during account creation or critical actions. Users perform a live face scan to sign a challenge, confirming their humanness without storing or transmitting biometric data. This process helps prevent automated abuse such as spam, fake accounts, and fraud by ensuring that only actual individuals can complete certain actions. The verification is seamless and privacy-preserving, enhancing user trust and maintaining the integrity of the platform while complying with data protection regulations.

Example 3: Secure Digital Signatures for Legal Documents

Face PKI enables authentication and signing of legal documents digitally. Users can sign contracts, affidavits, and court documents with cryptographic signatures derived from their face. The recipient can verify the signature's authenticity, ensuring the document was signed by the legitimate party, and not just by someone who had access to the parties' devices. This enhances the security and integrity of legal processes, reduces paper usage, and speeds up transaction times.

Example 4: Secure Communication for Organizations

Face PKI can secure communication such as emails, messages, files, etc., by encrypting the sensitive information or signing them digitally. Recipients can verify the sender's identity and the integrity of the message without accessing any biometric data and utilize their own private key to decrypt it or using the public key of the sender to verify the signature. This practice prevents phishing attacks and unauthorized access to confidential information, enhancing corporate security and compliance with data protection regulations.

Example 5: Secure Access to Accounts and Apps

Banks and financial institutions can use Face PKI to secure online and mobile banking. The companies can use Face Certificates to authenticate transactions and access accounts. This method provides strong, non-repudiable authentication without requiring passwords or physical tokens. The private key derived from the user's face ensures that only the legitimate account holder can authorize activities, reducing fraud and enhancing security.

Example 6: Streamlined eKYC Verification for Financial Services

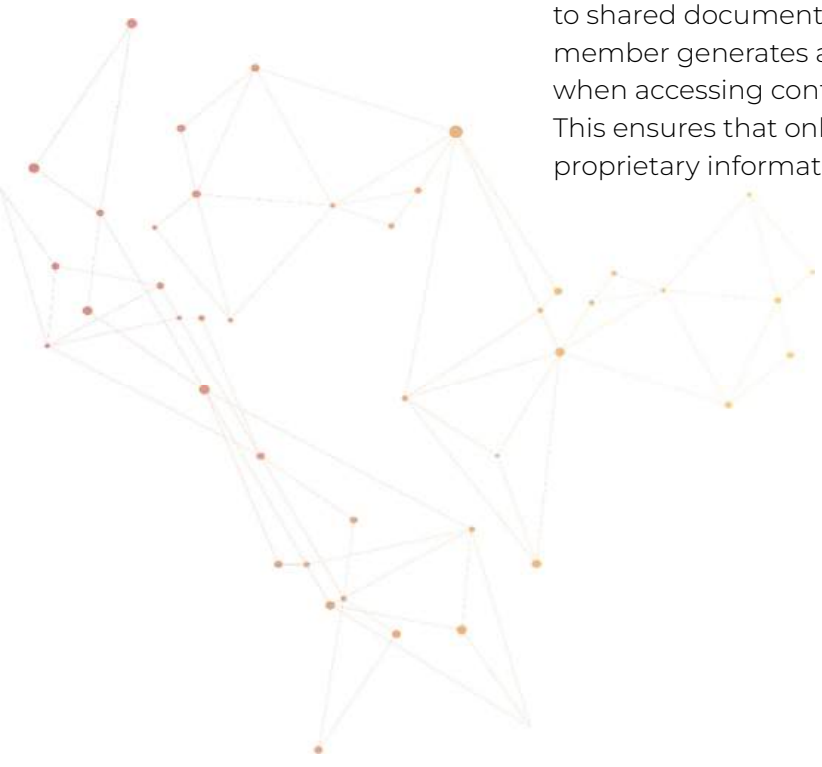
Financial institutions can use Face PKI to simplify electronic Know Your Customer (eKYC) processes. Customers perform a live face scan to generate a Face Certificate with their verified identity attributes. Banks authenticate these customers securely without storing or transmitting biometric data. This accelerates onboarding, reduces fraud risk, and ensures compliance with regulations. The process is seamless and privacy-preserving, enhancing user trust and improving the overall customer experience.

Example 7: Government Services Authentication

Government agencies can implement Face PKI for citizens to securely access online services, such as tax filing, benefit applications, and personal records. Citizens use Face PKI to authenticate themselves, ensuring that sensitive information is only accessible by the rightful individual. This improves the efficiency of service delivery while maintaining high security standards.

Example 8: Secure Collaboration in Corporate Environments

Teams working on sensitive projects can use Face PKI to control access to shared documents and communication channels. Each team member generates a Face Certificate to authenticate their identity when accessing confidential files or participating in secure discussions. This ensures that only authorized personnel can collaborate, protecting proprietary information and preventing unauthorized disclosures.



SenseCrypt DLT Protocol

The SenseCrypt Distributed Ledger Technology (DLT) Protocol, a world's first, integrates biometric verification into blockchain applications without storing or transmitting biometric data.

The technology allows the user to securely store their Verifiable Credentials in an identity wallet and present them effortlessly in a Verifiable Presentation when needed. SenseCrypt DLT goes a step further with Face Verified Credentials and Face Attested Presentations. Now, issuers can grant credentials only after face verification – without transmitting or processing any biometric data. Verifiers receive cryptographic proof that it was the user who performed the transaction.

The SenseCrypt DLT Protocol enables seamless integration with blockchain-based identity systems and existing decentralized identity frameworks, providing strong authentication without compromising the decentralized nature of blockchain systems.

Key Features

- **Trusted Witness System**: Validates transactions using Witnessed Credentials, enhancing trust in decentralized environments.
- **No Biometric Data on Ledger or within Credentials**: Ensures that sensitive biometric information is not stored on the blockchain or within credentials, preserving privacy.
- **No Transfer of Biometric Data between Parties (Issuer, Wallet, and Verifier)**: Issuers and verifiers never receive the biometric information yet can verify that the presentation has been made by the correct "face".
- **Enhanced Security**: Addresses the challenge of trusting digital wallets and identities in decentralized applications.
- **Non-Correlatability**: Privacy is preserved without sacrificing security, as all presentations and verifications are private and unique, with zero correlatability. This ensures the core principle of decentralized architecture is maintained.

Face-Based mTLS Protocol

Forget about usernames, passwords, and OTPs. In the future, your internet connection could be encrypted with your face! And that too at the most fundamental layer – the Transport Layer.

The Face-Based Mutual Transport Layer Security (mTLS) Protocol is an innovative approach to securing internet connections through face-based authentication. Traditionally, in mutual TLS (mTLS) protocols, a server verifies a client's certificate via a CertificateVerify message during the TLS handshake. This message includes a signature of all preceding handshake messages, signed using the private key linked to the client's certificate.

In the Face-Based mTLS Protocol, the client certificate is replaced with a Face Certificate. To perform a mutual TLS handshake, the client must generate a private key that can only be created using the face of the Face Certificate holder. This unique key is then used to sign the CertificateVerify message.

By securing all applications, browsers, and other connections to the server with facial authentication, this protocol ensures that websites and companies are interacting with a live human rather than a bot or AI agent. This secure technology places humans at the center, enabling them to better control and trust their online experiences without sacrificing privacy.

Potential Advantages

- **Eliminates Traditional Credentials**: Could replace usernames, passwords, and OTPs, simplifying the authentication process.
- **Integrated Security**: Embeds biometric authentication directly into the mTLS handshake at the transport layer.
- **Strong Protection**: Enhances security against man-in-the-middle attacks and unauthorized access.
- **Privacy Preserving**: Although the face is used to generate the private key, it is never revealed or sent to a third party.

Seventh Sense Differentiation

Seventh Sense operates in the competitive field of biometric authentication and identity verification, facing competition from established players and innovative startups alike. However, SenseCrypt solution is well ahead of its competitors. The key differentiators are:

1. **Privacy-First Approach**: Unlike many competitors that store biometric data, SenseCrypt's **"0% Biometrics - 100% Privacy"** approach eliminates the need for biometric data storage, significantly enhancing user privacy and simplifying GDPR compliance. A clear advantage over all competitors.
2. **Face-Based PKI**: SenseCrypt's unique Face-based public key infrastructure sets it apart by combining biometric authentication with cryptographic security, offering stronger protection against identity theft and ensuring non-repudiation in transactions.
3. **Post-Quantum Cryptography**: By integrating post-quantum algorithms like CRYSTALS-KYBER and CRYSTALS-DILITHIUM, SenseCrypt future-proofs its security against potential quantum computing threats, a feature not commonly offered by competitors.
4. **Offline Verification:** The ability to perform offline, distributed face verification through QR codes gives SenseCrypt eID an edge in scenarios with limited connectivity.
5. **Versatility**: SenseCrypt's technology can be applied across various use cases, from financial services to government applications, offering a more comprehensive solution than many specialized competitors.
6. **Compact Size**: SensePrints are approximately five times smaller than traditional biometric templates, offering efficiency advantages in usability as QR Codes, storage and transmission.
7. **Integration with Existing Systems**: SenseCrypt's technology compatibility with standard protocols like SAML 2.0, OAuth 2.0, and FIDO 2.0 allows for easier integration with existing identity and access management infrastructures, unheard of from biometric providers.
8. **Continuous Innovation**: Seventh Sense's focus on the intersection of machine learning and cryptography drives ongoing innovation, helping it stay ahead of evolving security threats and market demands, again as the sole company at the intersection of both.

Futureproofing - Post-Quantum Cryptography Integration

By implementing PQC, Seventh Sense addresses a critical vulnerability in current cryptographic systems. Many of today's encryption methods, particularly those based on factoring large numbers or solving discrete logarithm problems, are vulnerable to attacks by large-scale quantum computers. Quantum algorithms like Shor's algorithm could potentially break these cryptographic systems, posing a significant threat to data security and privacy.

After many years, the initial standards for Post-Quantum Cryptography were released in August 2024. This marks the ideal time to begin integrating these algorithms. Not only have we implemented the standards, we've also open-sourced the algorithms and their implementation to the SSL Certificates working group (IETF LAMPS group). Contributing to the first cryptographic foundation for the next generation of certificates that will secure the internet. These certificates also form the basis of our current and future Face PKI.

The integration of PQC is unique and critical feature that future-proofs the platform against potential threats as quantum computing technology advances.

The platform adopts the quantum-resistant algorithms selected by the National Institute of Standards and Technology (NIST). Specifically, Face PKI implements:

- CRYSTALS-KYBER: A module-lattice-based key encapsulation mechanism, designed to resist attacks from both classical and quantum computers, providing secure key exchange for encrypted communications.
- CRYSTALS-DILITHIUM: A module-lattice-based digital signature algorithm, ensuring the integrity and authenticity of digital signatures in a post-quantum environment.
- SPHINCS+: A stateless hash-based digital signature algorithm, providing an additional layer of post-quantum security for digital signatures.

In line with the recommendations from the European Union Agency for Cybersecurity (ENISA), Face PKI supports a hybrid approach to cryptographic agility by integrating traditional cryptographic algorithms with post-quantum algorithms.

The adoption of PQC standards allows Face PKI to offer:

- Long-Term Security: Data encrypted today will remain secure even if powerful quantum computers become available in the future.
- Compatibility with Existing Systems: The PQC algorithms are designed to work within current cryptographic frameworks, allowing for smoother integration and transition.
- Resistance to Both Classical and Quantum Attacks: The chosen algorithms provide protection against both traditional and quantum-based cryptanalysis.

Conclusion

SenseCrypt's innovative use of SensePrints – zero-knowledge face proofs, and secure Face Certificates creates a robust framework for biometric authentication that prioritizes user privacy and aligns closely with GDPR principles.

By design, the system minimizes data collection, ensures purpose limitation, and provides strong security measures, making it a privacy-preserving solution for identity verification in the digital age.