

**When you really need to
know who they are.**



Authenticating people, not just credentials.

3-Factor Dynamic Digital Signature
(DDS-3) for end-to-end proof positive
identity assurance.

First, we actually authenticate people, not just credentials

Multifactor Authentication

The National Institute of Standards and Technology categorizes user authentication methods as three factors: secrets (something you know), biometrics (a unique physiological characteristic) and tokens (physical object).

How SensiPass® is Different

While there has been much innovation in the biometrics and tokens space, we have focused our innovations in the secrets space, providing an interactive, registered secret that serves as a platform to augment various types of tokens and biometrics.

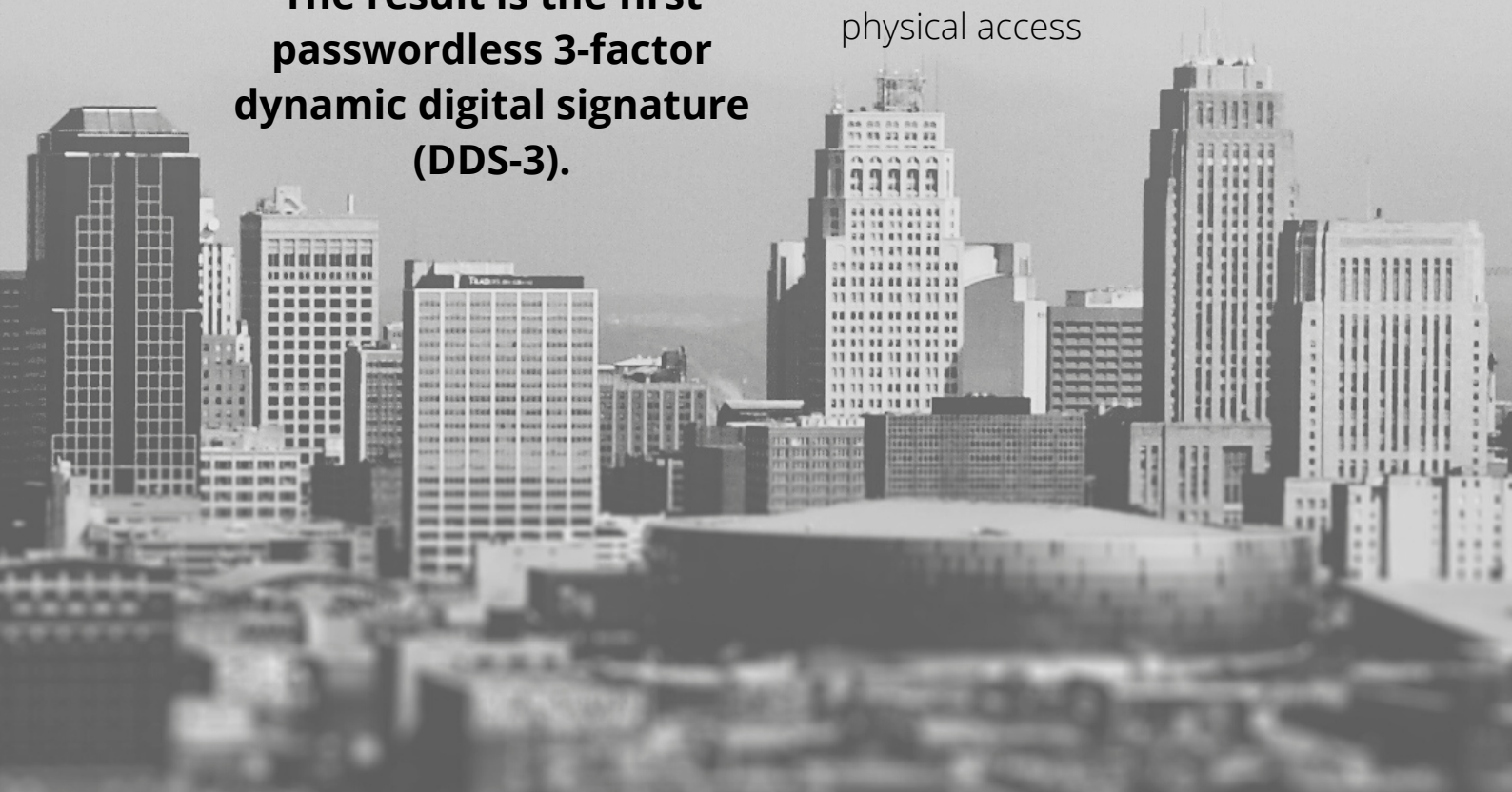
The result is the first passwordless 3-factor dynamic digital signature (DDS-3).

Our approach to identity verification disrupts two main flaw-causing norms in the industry:

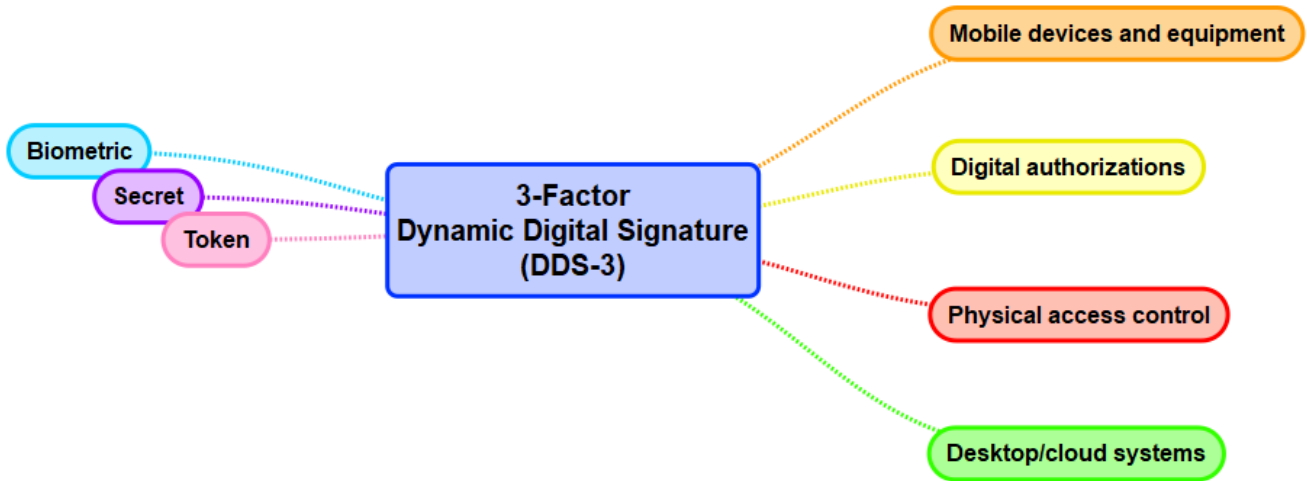
- The use of passwords and usernames somewhere in the authentication system
- The use of only two of the NIST-defined three factors of authentication in any system

Result of our patented approach:

- Bulletproof credential databases
- Integrated, secure credential self-resets
- Un-shareable credentials
- Proof-positive identity assurance
- Single ID for mobile, desktop and physical access



3-Factor Dynamic Digital Signature (DDS-3)



Our application can be easily deployed as a single mobile solution to easily authenticate users to mobile applications:

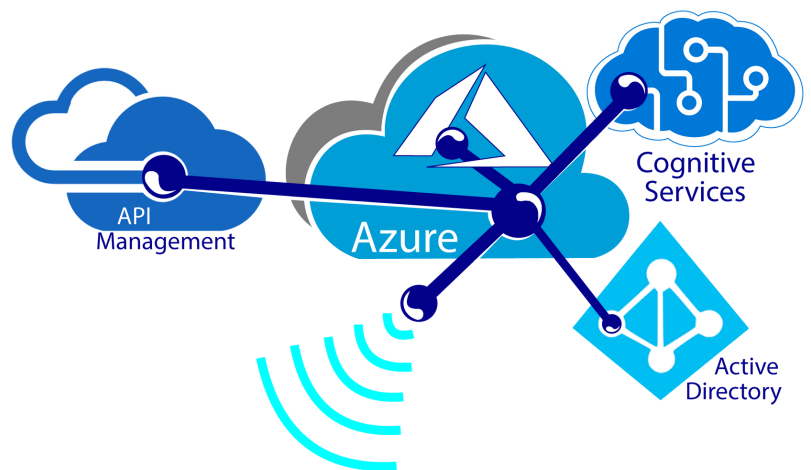
- Digital and physical access
- Digital Signature for ID checks
- Authorizing transactions.

We have built solutions around cloud-only, client-only and mixed architecture requirements:

SensiPass has designed specialized solutions around their interactive platform for several use cases including trusted cargo, augmented and mixed reality, and identity proofing for the on-boarding of customers.

Sensipass Access Control

1. User scans locking mechanism for ID using Sensipass equipped scanner
2. User authenticates the (un)locking transaction using Sensipass API via smartphone, tablet, or other integrated device
3. Sensipass data and the container/lock ID are sent to the cloud for processing
 - a. Authentications server/container via RTICM locking system
 - b. Alternatively, the ID and Sensipass data can be sent directly to auth server via gsm scanner
4. Results from processing relayed back to the container/lock mechanism
 - a. Alternatively, the result can be sent directly to the scanner device and unlocked by authenticated user locally on scanner



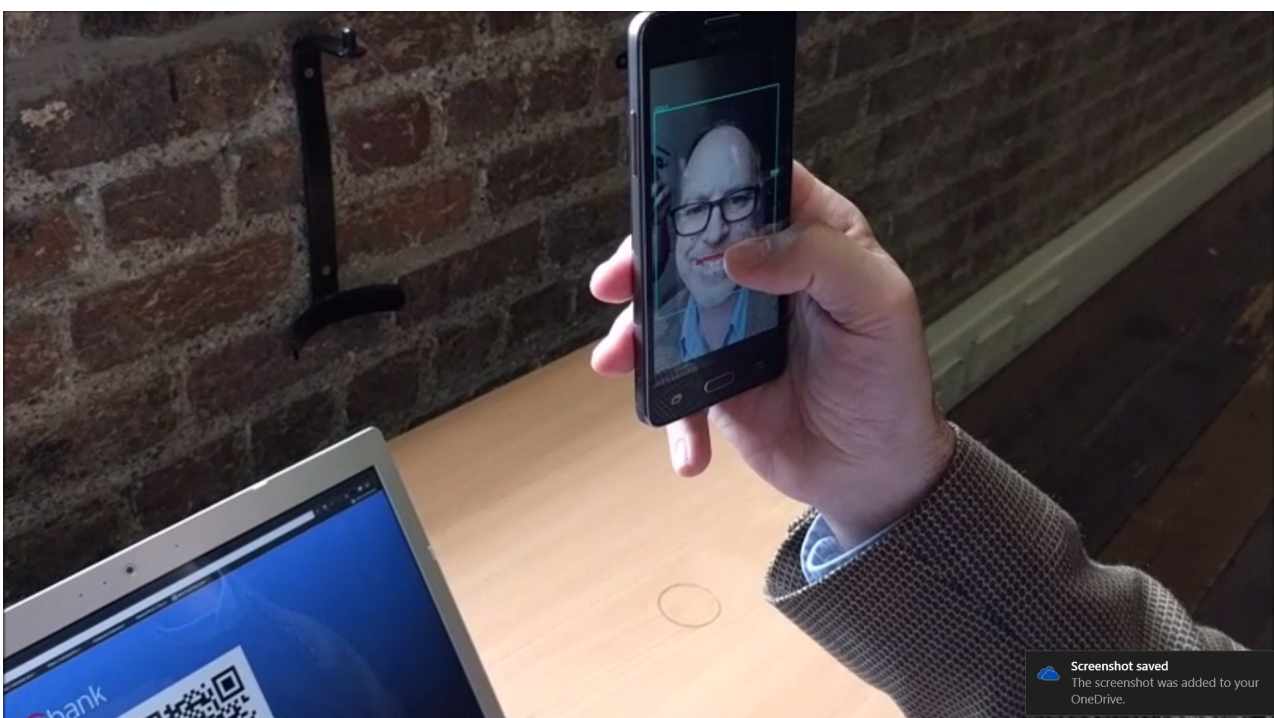
SensiPass Features ⇒ Benefits

Feature

- SensiPass products have **no need** for the username and password/PIN paradigm **anywhere** in the identity and access management (IAM).
- SensiPass provides a **highly entropic secret**, or knowledge factor, the secret interaction with a user-prescribed object.
- SensiPass combines **all 3 authentication factors** into a single, simple to use authentication method.
- The human, interactive nature of SensiPass products inherently provides **several liveness tests** that cannot be shared or easily replicated by others.
- Single digital signature that can be implemented as a **self-serve federated ID**.

Benefit

- **Eliminates** the most popular attack vector for cybercriminals -the password database- as we can **reject** exact matches and trigger actions.
- Results in a highly sophisticated 2-factor digital signature; **3FA** when combined with our blockchain-based dynamic token.
- As **each authentication factor requires a different type of hacking approach**, the complexity of hacking the system becomes a much greater burden for criminals.
- SensiPass cannot be replayed, nor shared to be used by others, effectively eliminating compromised, careless or malicious **insider threats**.
- **Eliminates the redundancy** of multiple identity and access systems for digital, physical and mobile access.



Solutions

Digital Access: SensiPass' core product. Access to systems including mobile apps, mobile access to websites, or other devices such as laptops/desktops/kiosks using the SensiPass Authenticator application.

Physical Access: Physical access cards do not prove identity. In much the same way SensiPass secures digital access, the SensiPass Authenticator secures turnstiles, gated facilities and SCIFs.

Digital Signature: At its core, SensiPass is a 3-factor dynamic digital signature and can be used for authorizing transactions, documents and sign trusted cargo with proof-positive identity assurance.

AR/VR/XR Login: *ImmersiveID*[™] is our patented product line for 3-factor authentication designed for securing user access to immersive environments, and can eliminate the need for peripheral devices, a weak link, in the authentication process.

Assured User Onboarding: SensiPass can overcome security risks associated with independent scanning of documents during the remote onboarding process for banks and other users.



About SensiPass®

SensiPass was established in 2013 to build upon and promote their patents and intellectual property related to digital identity. Based in Dublin, Ireland, SensiPass has developed partnerships in 11 countries and a physical presence in the United States.

SensiPass understands and acknowledges that multi-factor authentication is not new to governmental and other critical enterprise computing systems. As security threats grow in number and sophistication, expanding the use of multi-factor authentication that is resistant to attack has become a renewed priority, especially for systems containing personally identifiable information, and mission-critical information or materials. While the security industry is only offering 2-factor authentication, SensiPass was designed as a 3-factor solution from inception, and without the vulnerabilities and problems of username/password combinations.

SensiPass® products are protected by patents and trademarks worldwide both issued and pending. Current information can be found on our website.



SensiPass®: A Very Different Approach to Human Authentication

SensiPass Ltd., 2nd Floor,
Digital Exchange, Crane Street
Dublin D08HKR9
+353 85 833 4477
NCAGE: SCSG5

SensiPass Inc.
3101 Wilson Blvd, Suite 240
Arlington, VA 22204
+1 202 412 0821
CAGE: 88RW9