Biometric, Multi-Factor Authentication
Protecting the Perimeter

Your smartphone can verify that you are who you claim to be in a matter of mere milliseconds. Why should it be any different with your apartment building's doorman? Or your office building? Or even when going through U.S. Customs?

The very same convenience you take advantage of on a daily basis — whether through fingerprint recognition, facial scanning, or even a simple passcode — is already more secure and reliable than waving hello to your doorman as you return from work. This is a testament to modern technology, but also a glaring issue for physical access security.

Security - both for private and public-sector organizations - is fundamentally about identity. Only the right individuals should have access to their authorized physical locations, and that requires real-time confidence that the people arriving, and departing are who they claim to be.

Yet for many organizations, verifying the identity of guests and registered personnel remains a persistent challenge. The vast majority of people constantly carry an advanced biometric capture and transmission device - their smartphone - in their pocket. Yet even as enterprise-level IT infrastructure advances, many companies still rely on vulnerable, imprecise, and highly manual processes for verifying the identity of individuals. Despite the fact that the mobile technology you and your employees are already using can provide the foundation for smarter, safer identity-based access management.

What's wrong with the status quo?

Traditional area and building security practices are familiar to anyone who has passed through customs, visited an office building, or entered a doorman apartment building in the past 20 years.

- Approach the security officer
- Give your name
- Provide a driver's license or equivalent
- The security officer checks your form of identification, with your face, against a guest list
- Officer calls your host to notify them of your arrival
- Once all steps are completed, you are alllowed to enter

Guests may only be provided a temporary sticker as a badge for subsequent identification, often with manually-generated and unreliable visitor logs, and low-resolution security camera footage providing the sole audit trail. Once inside the secure perimeter, guests must be escorted through RFID-secured doors by security or a chaperone, with no way of tracking which doors they have passed through or where in the facility they have attempted to go. Guest identification badges have achieved a remarkable level of inertia at the enterprise-level since the technology was developed more than three decades ago. While still entrenched across the marketplace, reliance on these outdated security methods in 2018 presents several security threats:

Insecure: Reliance on human eyes for verifying the identity of a guest using a driver's license or passport is notoriously unreliable. Individuals are highly susceptible to distraction, social engineering techniques, or fake credentials. With high-quality fake IDs available on the dark web complete with scannable barcodes and UV-ink even highly-trained security personnel are vulnerable to deception.

Easily Lost: RFID cards allowing employees or known visitors to bypass are frequently lost or misplaced, with credentials remaining active until an employee self-reports the loss. In the interim, whoever finds the badge has full access to your facility with just the tap of a keycard, putting your people and resources at risk

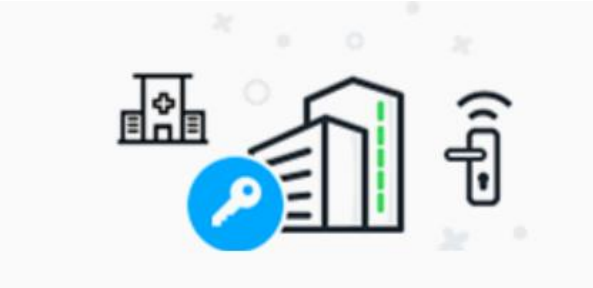
Single-Factor: Traditional access control systems grant access to badges, not to individuals. Credentials all too often allow individuals to escape individual scrutiny and identity verification processes regardless of whether the person holding it is the actual badge holder or an impostor. Robust security requires a mechanism to match the identity credential to the user.

Vulnerable: Many widely-used RFID badges are vulnerable to remote scanning and cloning from distances of up to three feet. With less than $1,000 worth of widely- available components, it's possible to wirelessly capture and duplicate an RFID badge in minutes. Don't let 1980s technology leave you vulnerable.

MOBILE IDENTITY ACCESS MANAGEMENT SOLUTIONS

Mobile identity solutions can be a valuable tool for companies looking to mitigate these issues. As with any critical enterprise infrastructure decision, though, achieving a balance of security, economy, and simplicity is key. Companies should keep a few critical questions in mind as they consider how best to move past legacy systems heavily reliant on manual checks and outdated technology:

How is this going to heighten security for my facility? The security of your facility should be top of mind when it comes to access control decisions. Don't settle for last-generation, single-factor authentication methods that leave your company vulnerable. Demand the latest in multi-factor, out-of-band authentication technologies.



How is this going to make my life easier? Physical access is just one of many systems corporate users must interact with on a daily basis. Look for solutions that offer integration beyond physical access control, from time and attendance to visitor management.

How well does the solution work for end users? Traditional, manual access control solutions are popular because they're simple, and users know what to expect. Users demand a fast, easy, and seamless user experience from replacement technologies, regardless of the security benefits. Multi-factor security shouldn't come at the expense of convenience.

How easy is the solution to implement? No two organizations are alike. Watch out for one-size-fits-all solutions that lack the flexibility required to meet your individual mix of system configurations and business requirements. The right solution should be a customizable product with minimal friction at implementation.

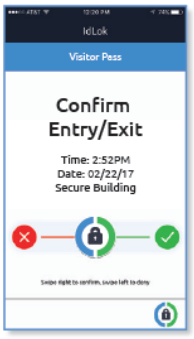
Does the solution scale? Identity is at the core of key challenges facing organizations across the public and private sectors. Expect a solution that can do more than just unlock doors. Secure any interaction or transaction with biometrics, create a cryptographically secure audit trail, and be notified of exceptions in real-time.

ENTER - ACCESS BY IPSIDY

Today the one thing we all have 24/7 is our smart phone. Advanced biometrics are embedded into everyday devices, and are being leveraged across the digital environment. It's likely that your company is already among the 75% of organizations either currently using, or considering implementing a "bring your own device" policy. In fact, chances are good that you're currently reading this white paper from a mobile device. These devices that we rely on for day-to-day productivity build the foundation for Access by Ipsidy, the next-generation of identity-based access management.

Protect the perimeter of your facility by deploying **Access by Ipsidy** with Bluetooth Low Energy (BLE) beacon technology, an end-to-end solution offering both flexibility and scalability. Provide a single solution for managing employees, residents, and temporary visitors and create both physical and virtual access points to monitor movement into and throughout doors or areas.

Replace vulnerable manual processes with the latest in facial recognition technology. Create a biometrically-signed and cryptographically secure audit trail.



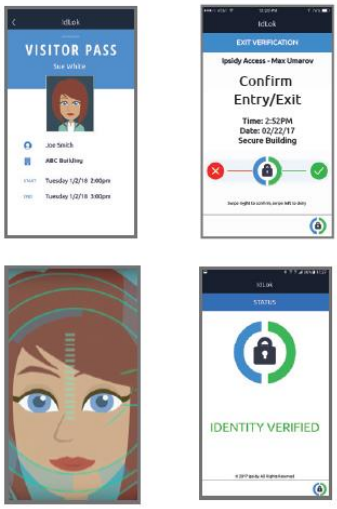
SECURE - With Access by Ipsidy, guarantee the identity behind every transaction with secure facial biometric matching. Eliminate the risk of lost, stolen, or shared RFID badges with the latest in multi-factor, biometric authentication technology. Protected from fakes or spoofs with liveness detection, and encryption using the latest 256-bit technology.

SIMPLE - Ditch closed, proprietary platforms requiring expensive, custom physical hardware installations and costly maintenance. Simplify with Access by Ipsidy, combining low-cost BLE beacons with cloud-based access management and smartphone applications.

CONVENIENT - Provide the peace-of-mind of biometric multi-factor authentication without sacrificing user experience. With Access by Ipsidy, beacons seamlessly trigger push notifications to the user's device, then it's just swipe, blink, and smile to authenticate! Employees and visitors alike will love seamless BYOD (Bring your own device) integration with support for the latest Apple iOS and Android devices.

FLEXIBLE - Get up and running immediately with our white-label "out of the box" app. Configure and manage your site(s) and their virtual access points or physical perimeter, users, user groups, monitoring locations, and user privileges in real-time from the Access by Ipsidy web portal. Monitor in real-time who is accessing your site from anywhere through our mobile Concierge application. Integrate outside systems effortlessly with RESTful APIs, and multilevel decentralized administration with central oversight.

ACCESS BY IPSIDY – HOST & VISITOR MOBILE APPLICATION



- Simple Biometric Verification Process
  - ✓ Beacon triggers push notification to phone
  - ✓ Host or Visitor swipes right to verify identity
  - ✓ Automatic, front-facing camera with liveness detection prompts user to capture face with just a blink and a smile
- Apple & Android mobile smartphone applications
- Host application offers convenient & secure Visitor Pass issuance
- Multiple 'family' accounts managed & verified in same application

ACCESS BY IPSIDY – CONCIERGE MOBILE APPLICATION

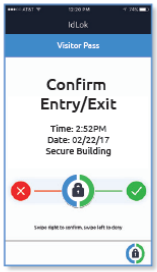
- Online enrollment of new users
- Real-time display of identity transactions
  - ✓ Stored and live capture facial images & demographics displayed
  - ✓ Color coded for pass/fail/incomplete identification status
- Exception processing
  - ✓ Re-trigger identity verification
  - ✓ Complete identity transaction: Capture user biometrics
  - ✓ Initiate identity verification (no smartphone)
  - ✓ Perform system overrides as needed
- Configurable screen layout to reflect facility & beacon configuration

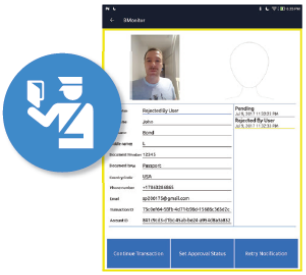
ACCESS BY IPSIDY – ADMINSTRATIVE PORTAL

Access by Ipsidy offers a full-service web-portal, with multi-level administrative roles. Site administrators can view and manage their site data or campus administrators can view activity across multiple sites. Convenient tools allow administrators to self-configure perimeter areas and define custom groupings of site access points, residents, employees and visitors. You can even track employee attendance by reviewing portal access logs. Access by Ipsidy lets you know with certainly who is where and when they arrive or depart.

SAFER, SMARTER PHYSICAL ACCESS MANAGEMENT

Traditional access control solutions are holding your organization back. Your employees and clients alike expect you to facilitate secure digital interactions, and most are already interacting with your assets and services via a mobile device. Mobile identity authentication solutions are a valuable opportunity for your company to enhance security and convenience while building trust.





Access by Ipsidy provides seamless and secure facility access control by leveraging the power of smartphone biometrics, the ease and flexibility of BLE beacon technology, industry-leading cryptography and physical access capability. Satisfy employees, residents, or visitors with a convenient access control experience, from their own device. Enhance security with true multi-factor authentication, real-time transaction reporting and exception processing, and biometrically-secured audit trails.

Break the mold and achieve safer, smarter physical access management with Ipsidy.