WHO ARE YOU? VERIFYING YOURSELF IN AN AGE OF IDENTITY THEFT AND FRAUD

UNISYS | Securing Your Tomorrow®

Who Are You? Verifying Yourself in an Age of Identity Theft and Fraud

Every day we present evidence of our identity – whether to conduct a transaction online or gain physical access to a facility, passing through airport security or crossing borders. It is not a stretch to say that "our identity is one of the most critical assets we have in our lives." Authorities and businesses have a commitment to make the lives of legitimate individuals a little easier in establishing their identity, while earning their trust by ensuring the highest standards of safety. Internally, organizations need to make the process of identity enrollment and verification simple, tamper-proof, cost-effective and sustainable by leveraging technology advancements.

When it comes to identity theft and fraud, most recent news accounts have focused on the avalanche of online data breaches and similar forms of cyber-crime. However, online data theft is just one component of identity compromises; forgery and identity theft in the physical realm is also a major cause of concern among government agencies, financial and healthcare providers, and other institutions that rely on positive, irrefutable physical identification. Meanwhile, victims of identity theft are denied services and suffer financial and legal harm when someone else hijacks their identity. Yet the systems for proving "who we are" are increasingly failing us. In the 2019 Javelin Strategy and Research Study, findings revealed that identity fraud in the USA alone affected 14.4 million individuals and resulted in a loss of $3.4 billion in stolen funds[i]. Similarly, 50% of all Social Security fraud is due to falsified multiple identities. Medicaid/Medicare, insurance companies, and government assistance programs are all seeing increased use of stolen or falsified ID to scam their systems.

Moreover, money lost is not the only issue with ID theft. Using false or stolen identities, criminals and terrorists compromise borders and threaten national security and safety in countries worldwide. The Institute of Economics and Peace reported in 2019 that two out of every three countries in the global terrorism index (103 nations), experienced at least one terrorist attack[ii]. Meanwhile, international criminal gang members using false or stolen identification move across borders with impunity.

Why Are Document Security Services Failing?

In the past, a photo ID and other documentation were enough to establish clear identity, but criminals and terrorists are now a step ahead of authorities by using advanced technologies. Document and photo forgery, once a specialized criminal skill, is now available to any malicious actor with a scanner, PC, and a high-end printer. While more sophisticated documentation features (such as hologram embedded photo IDs and paper) took a step in the right direction, well-funded fraudsters now have equal access to this technology, upping the ante on fraudulent documentation and its detection. Chip-embedded documents and cards are the latest effort to secure physical documents, but even these methods are subject to sophisticated attacks. Furthermore, purely physical documents—hologram passports, chip-embedded documents—are proving to be increasingly limited in a world where transactions and identifications are increasingly conducted online.

Digital Identities Routinely Fail Too

To protect online accounts and IDs, too many systems continue to rely on passwords and personal identification numbers (PINs) alone to authenticate users. Both fail on a regular basis, and the reasons are well documented: passwords and PINs can be hacked or stolen, and most users do not follow password and PIN best practices. Too many rely on easy-to-guess passwords ("123456" is still the most frequently hacked password, four years in a row!)[iii], or users write down passwords that are too complex to remember and require frequent resets. As many personal documents and background data are also in electronic formats, there is a booming black market for selling personal information. For example, according to a 2017 Experian report, "Here's how much your (US) personal information is going for on the Dark Web"[iv]:

The Cost of Identity Documents on the Dark Web	
Social Security Number	$1
Driver's License	$20
Passports (USA)	$1,000-$2,000
Medical Records	$1-$1,000

The Rise of Two-Factor Authentication

In response to the rise in ID theft and compromise of passwords and PINs, two-factor authentication has become the new minimum standard in identity protection. In summary, two-factor ID must be based on two of three potential authenticators:

1. Something you physically have in your possession (a phone, electronic token, etc.),
2. Something you know, such as a password, PIN, or personal fact (what was your high school mascot, for example), and
3. Something that is *you*, such as a fingerprint, facial image, or iris scan.

Most of us are now routinely using two-factor authentication when we log onto our bank accounts, for example—signing up for our online account requires authenticating the machine we'd use for access (PC or phone, usually) and the security system then embeds a security token on the device to positively identify it (something you own and have with you) for access. This is augmented with a password, PIN, or even a fingerprint—the second factor.

But as we've already noted, passwords and PINS are routinely compromised—and physical devices such as phones or hardware tokens can be lost, stolen, or cloned. "Secret questions" such as your high school mascot, meanwhile, are not all that secret in the open world of social media where personal history and information are on display for the world to see. Additionally, as an example, Facebook routinely has "games" that ask for answers to these questions, and a high percentage of users still fill in the answers. But what about fingerprints? facial recognition?

Biometric Flaws?

We leave fingerprints behind on everything we touch. There are well documented spoofs of fingerprint recognition on phones and even dedicated fingerprint readers[v]. As for facial recognition, (often used on PCs, phones, and laptops) a recent research paper suggests silicone masks can spoof some of the most prevalent facial recognition software[vi]. Meanwhile, reliable, consumer-market iris scans are not yet available, although some phone manufacturers have had limited success deploying them. However, all biometric technology is improving in speed, accuracy, and affordability, and biometric ID authentication is less susceptible to wholesale compromise of identities—such as hacking a database of hundreds of thousands of IDs and passwords. In contrast, spoofing or replicating even a handful of biometric IDs would be exponentially more difficult for criminals.

Other Tangible Costs of Current ID Systems

Aside from the tangible costs associated with ID theft and fraud from failed authentication systems, there are also very real capital and operating expenses associated with many current ID systems.

First, implementation of these ID systems often requires a significant investment in software, hardware, training, and integration with existing security and IT systems. Depending on the level of vendor-centric components required, organizations may need to spend considerable time and money implementing these identity authentication systems. Secondly, due to the proprietary nature of the solutions, organizations are solely dependent on the chosen vendor for any future upgrades or potential improvements in technology. This vendor lock-in itself may put security at risk—either through outright failure or the inability of the chosen vendor systems to quickly respond to new or emerging threats. This can put the buyer in an impossible situation, where the organization's requirements exceed the capability of the product.

Furthermore, given the time and effort required for registration, and potential cost to individuals to obtain physical identification tools such as passports and fingerprint-protected devices, many people simply "opt out" of the process entirely. The "friction" inherent in using the provided system pushes them away. They never register in systems designed to benefit them. Cost, time, and the hassle of enrollment contribute to non-participation.

Digital ID presents an even greater hurdle: According to a 2019 Digital Guardian study[vii], a survey of 1,000 adults revealed that the average user has almost 90 separate digital accounts—many of which deploy the same PINs, passwords, and biometric signatures in an effort to streamline their online lives. In other words, if one account is compromised, they are all now vulnerable to compromise. Meanwhile, the sheer number of accounts means that, on average, most online citizens must reset or retrieve a lost password or PIN every week.

Finally, setting up or recovering lost passwords and PINs, incomplete or erroneous biometric data, and reliance on only two factors for ID authentication introduces potential security lapses and lost productivity for organizations and the clients they serve.

Agility Is Needed to Deliver the Best Identification Systems

Clearly, new approaches are required to reduce theft, fraud, and falsification. Identity assurance is an arms race—yesterday's best practice is today's security flaw. The hackers have more time, and zero restrictions to get into our credentials, and ruin our credit and digital reputation. The new standard requirement is identification systems that provide defense in depth through multiple, agile use of multiple authentication technologies—allowing organizations to quickly respond to new threats by mixing and matching technologies in response to new threats. An agile and highly fluid approach to ID assurance eliminates large-scale exploitation of single vulnerabilities and makes hacking multiple identities financially unfeasible for criminals. The cost of attacking agile, adaptable security systems far outstrips the value of acquiring the data.

To meet these requirements an identification system must not rely on older, potentially compromised authentication solutions. Identities based on passwords, PINs and physical documents that can be forged, stolen, or altered are the weakest links in combating identity fraud. Leading security experts also know that establishing identities based on two factor authentications (what an individual "knows or has") is insufficient protection against sophisticated identity thieves.

Security system operators need systems that can easily use multiple points of identity authentication to automatically respond to new threats.

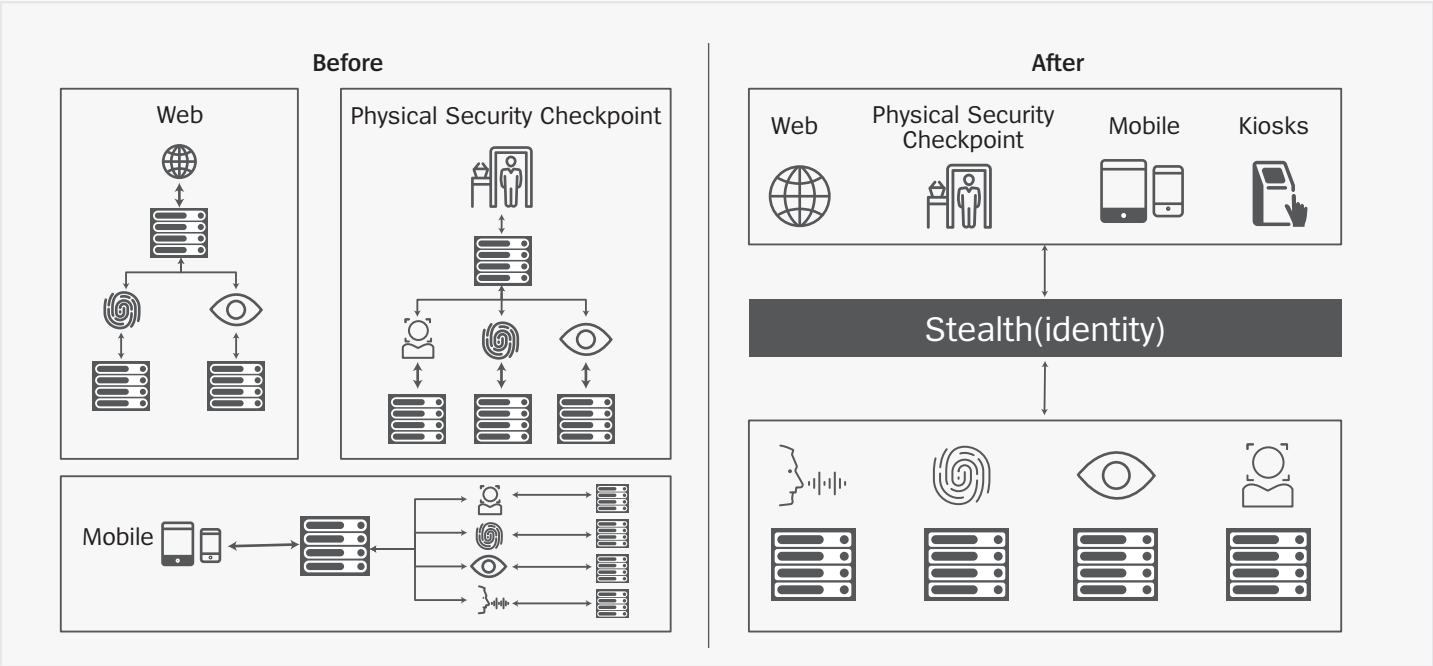
Fraud Protection and Stronger Security with Stealth(identity)

Unisys has almost 20 years of experience in delivering field-tested and proven identity authentication systems. Its latest product, Stealth(identity)™, delivers all security authentication best practice requirements through a combination of an open technology architecture derived from extensive client experience, and the latest innovations in biometric modeling. For example, one current client, a popular cruise line, uses facial recognition on its voyages to check guests onboard and during off ship excursions. The process is quick, requires no physical IDs, and greatly eases the burden of authenticating thousands of guests at ports. In addition, adding enhanced, crisis-specific biometric scans, such as checking temperatures to screen out those infected with a communicable disease such as COVID-19, can help our workers return to work as safely as possible.

Stronger ID Systems Using Multimodal Biometrics and Behavior

As we now know, single-factor (unimode) biometrics such as fingerprints and facial recognition are not adequate. Unisys Stealth(identity), however, uses the latest multi-biometric and behavioral identification systems in tandem to eliminate the chance of forgotten, borrowed, or stolen identities.

The Stealth(identity) Advantage



In current ID systems, each authentication method requires separate enrollment and verification—each using its own specific and often proprietary systems. Stealth(identity), however, is an open-architecture, multi-modal authentication system—users only need enroll once. From then on, they enjoy the security afforded by multi-factor authentication from a single repository of stored IDs. This dramatically reduces friction. Additionally, the number of available ID factors that Stealth(identity) supports is extensive and growing, and Stealth(identity) will interoperate with any of them, contributing to the avoidance of "vendor lock in". Voice recognition, fingerprints, iris scans, facial recognition, and an ever-expanding list of behavioral and physical traits can be enrolled into each customer's Stealth(identity).

Unlike unimode biometrics or two-factor authentications, Stealth(identity) delivers multiple layers of defense not easily or *profitably* spoofed. It delivers universal coverage of all citizens or clients with no gaps in coverage and its ID technology is not susceptible to single-factor errors or fraud.

Improved Productivity Through Automated, High-Volume, Near-Perfect ID Verification

Stealth(identity) also streamlines any organization's ID processing. Current Unisys clients enroll literally thousands of users per hour using its Stealth(identity) Fusion Engine, equipped with the most sophisticated accuracy determination algorithms delivering near-perfect identification accuracy through combining multiple biometric scores. Near-perfect identification accuracy means almost zero failure-to-enroll (FTE) and failure to match rates (FMR).

The result is far less user frustration, far shorter wait times, and extremely efficient and accurate ID verification for any organization—from online retail to high-volume physical ID checks, such as border crossings. Our "register once, use multiple times" approach to identity management can result in dramatic increases in efficiency across multiple uses in any enterprise.

Streamlined User Enrollment

While using a single identity repository cuts down on the creation and use of multiple accounts, Stealth(identity) also streamlines its own account enrollment and easily integrates with other ID verification systems. It can verify the legitimacy of an individual at the time of enrollment through integrated identity proofing or utilize its built-in, standards-compliant workflow engine to add custom background check routines. Automating the enrollment process dramatically cuts down on enrollment time, cost and reduces failure-to-enroll (FTE) rates. The registration process can also reduce fraud by de-duplicating biometrics—it checks each new enrollment against previously captured biometrics.

The result is reduced enrollment processing time and again, far less user frustration. This automation dramatically reduces and simplifies processing compared to current labor-intensive alternatives. Additionally, enrollment can be accomplished remotely, avoiding the need to travel to an office or other site to be enrolled, which in this time of Covid-19, will help us keep our people safe and healthy, with the minimum of friction.

Open Architecture and Plug-And-Play Integration Ends Vendor Lock-In

Using the latest technology, organizations can add new biometric, behavioral, and enrollment criteria whenever the need arises. They preserve investment in their systems and can integrate Stealth(identity) with their current and any future business and management systems.

Stealth(identity) integration also extends to system management. Operational complexity and administration costs are dramatically reduced with Stealth(identity)'s streamlined management console for all biometric types. The Stealth™ console integrates with any Common Biometric Exchange Formats Framework (CBEFF) compliant backend biometric processing system, thus creating one biometric security infrastructure.

Fast-Track Deployment

With its combination of open architecture and pre-configured options, Stealth(identity) can integrate quickly with any organization's current identity authentication systems. Organizations can jump start their implementation with easy-to-deploy pre-packaged functionalities such as multi-modal biometric enrollment processing, case adjudication, authentication, identity lifecycle management, common administration, and integrations with leading third-party biometric recognition and biometric devices.

In addition, organizations can easily customize and extend the system with application integration APIs. Unisys also provides expert professional services to help organizations avoid pitfalls in early design decisions and quickly customize and extend their biometric identity management system.

Stealth(identity) Use Cases

Unisys Stealth(identity) is a universal solution to irrefutable identity authentication.

For the enterprise, Stealth(identity) offers out-of-the box solutions that immediately improve e-commerce and access controls. Examples include:

- **Step-up authentication:** Access to sensitive information, or attempts to transfer large amounts of money require a secondary, biometric authentication.
- **Password reset:** By verifying the identity of an end-user with biometrics, self-service password resets can be accomplished without call to the help desk.
- **Enhanced physical access controls:** Integrated with entryway security systems, a biometric solution can offer a dramatic improvement in security over card-based access, as well as offer extra convenience for employees.
- **Paperless workflows:** For example, in an airport environment, a single biometric-based identity management solution could allow passengers to check in, pass security and customs, and board, without presenting a single piece of paper or mobile phone screen.

The examples shown above demonstrate how Unisys identity management solutions are unique in the verified identity ecosystem in that it solves ecommerce problems for the enterprise, as well as high-volume, high traffic public sector implementations. Such public sector use cases include:

- **Border security:** Governments can use Stealth(identity) to quickly process thousands of individuals per hour using face, voice, iris, fingerprint, and other biometric recognition. This can eliminate countless labor-intensive ID checks that in themselves may not provide adequate authentication.
- **Citizen registry:** Registrations can become nearly effortless as enrollment would entail a simple one-time scan of multiple biometrics. Automated systems reduce manual labor and eliminate fraudulent duplication or theft of identity.
- **Healthcare registration:** Eliminates repetitive manual ID checks and ensure proper identification throughout a patient's health procedures, from initial service registration to final billing. Biometrics of increasing sophistication do not require patients to fumble for PINs and passwords in critical care situations where every moment counts, especially if a patient is incapacitated.

Unisys Commitment to Identity Rights

Stealth(identity) provides a nearly limitless number of authentication technologies from which our clients can choose. As such, we are committed to facilitating our clients ability to choose which methods best serve their customers and citizens and aid in protecting their privacy rights. With Unisys, clients can deploy superior irrefutable identify systems yet protect individual privacy:

- Unisys is here to protect national, financial, personal and physical security as evidenced by our Unisys Security Index™ which reflects our overall mission. View the current survey here, which annually tracks citizen and worker concerns regarding online and offline security.
- As Stealth(identity) is designed to be multi-modal in nature, it is gender, color and policy-neutral as we track not only face but also voice, fingerprint, iris, behavioral identity, and other factors.
- Unisys doesn't own the biometric data used in authentication... our clients do. We facilitate the capturing, cleansing, encrypting, integrating, and analysis of this information on behalf of our clients for the purpose of national, financial, personal and physical security.

Conclusion

Current identity authentication methods—online and off, are failing to offer adequate protection of their identities and access to their important assets. Citizens and clients are subjected to too many enrollments. Passwords and PINs are now attack surfaces. Single biometric or even two-factor authentication is not secure enough. Single enrollment, multimodal biometric solutions such as Stealth(identity) are the future of identity verification. Its irrefutable identity authentication capabilities, on their own, solve most ID security problems. Yet the same feature set that delivers its superior ID security also enables faster processing, easier enrollment, and an extensible path to even better protection in the future.

References

[i] "019 Identity Fraud Study." Javelin Research. February 2019.
https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

[ii] "2019 Global Terrorism Index," Institute for Economics and Peace.
http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf

[iii] "The Worst Passwords of 2018." Security Magazine. December 17, 2018.
https://www.securitymagazine.com/articles/89694-the-top-100-worst-passwords

[iv] "Here's How Much Your Personal Information is going for on the Dark Web" Experian, February 2019.
https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[v] Levin. "Why Scanning Your Fingerprint Could Cost You Your Privacy." Inc. May 23, 2017.
https://www.inc.com/adam-levin/why-scanning-your-fingerprint-could-cost-you-your-privacy.html

[vi] Battacharjee, et al. "Spoofing Deep Face Recognition with Silicone Masks." Conference paper. October 2018.
https://www.researchgate.net/publication/329118426_Spoofing_Deep_Face_Recognition_with_Custom_Silicone_Masks

[vii] "Security Habits are Improving," Digital Guardian, December 2018.
https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic

For more information on Stealth(identity) visit www.unisys.com/sid

To speak to a Unisys representative about Stealth(identity) consulting services contact stealth@unisys.com

---

For more information visit www.unisys.com

05/20

20-0235