UNISYS

It's All About Strong Authentication

uLogon Biometric Authentication Solution

Protect business interactions and user identities with superior biometric authentication

Today's Authentication Reality:

Passwords Are Not Secure Enough

In today's business environment, an organisation's authentication system must enable its security administrators to verify user permissions before granting access to corporate data and monitor user activity through various logging mechanisms.

But the recent surge in high-profile security breaches has exposed the vulnerabilities of certain authentication mechanisms. This is particularly true for organisations that primarily deploy usernames and passwords for authentication purposes.

The problem with passwords is that a simple password can often be guessed or hacked, and a complicated password is inconvenient and difficult to remember. Furthermore, every forgotten or compromised password results in lost employee productivity and an increase in help desk support cost.

To achieve comprehensive information security and overcome the weakness of passwords, businesses need to deploy strong authentication solutions that deliver security, efficiency and control in a cost effective manner. The question is – is it possible?

uLogon: Your Hand is the Password

Enable Secure Access to Windows Desktops / Workstations

Unisys uLogon solution strengthens the authentication process by requiring an additional biometric feature – palm veins. Compared to other biometric technologies, the palm-vein method is traceless and absolutely non-invasive. At the same time, multiple mechanisms are in place to protect the personal privacy and fulfill legal and compliance requirements.

Using biometric specific readers, the uLogon software allows users to execute automated session engagement and disengagement interactions (Log-On, Lock, Unlock, Log-Off) with the network on their Windows workstations. This process ensures that users are indeed who they claim to be.

The uLogon authentication approach based on who you are (biometrics) is impossible to hack but convenient enough to identify and track individual users for future audits.

uLogon: Real World Application

Swift, secure access to shared workstations in multi-user environments

To swiftly and adequately serve customers, many businesses today need open (public) workstations. Banks, healthcare clinics, and manufacturing and shop floors require workstations/desktops that facilitate seamless access to records and critical applications.

But in choosing speed over security, IT administrators often create generic login credentials for these workstations, relying on user discretion for protection. Furthermore, when users fail to close their applications or simply leave the workstation without logging off, it can expose sensitive data to unauthorised users. As a result, these vulnerable workstations:

- Create security gaps and compliance issues
- Make it difficult to record the activity of individual users for future audits

The uLogon biometric authentication solution takes care of this by validating identities using palm-vein biometrics. The solution enables unique identification of multiple users on the same workstation without compromising on security.

Furthermore, the uLogon software takes care of traceability and control issues by logging the activities of individual users and preventing unauthorised access.

How it works

The uLogon solution works on a role-based access mechanism. Role-based access control takes the privileges associated with a user and maps them directly into the systems used for accessing IT resources. On implementation, it allows users to carry out activities - and only those activities - permissible by their role.

The solution is easy to implement and operates on the self-enrollment concept. Using a hand vein sensor, the uLogon software allows users to self-enroll on any Windows workstation by storing the encrypted vein image in the identity store. It offers:

- Kiosk version for shop floor environments
- Point of Sale (POS) & ATM versions
- Option of using a contactless smartcard in case use of biometrics is prohibited due to local legislation or other reasons

Key Benefits

By implementing the uLogon solution, organisations can allow legitimate users to access sensitive data anytime, anywhere. Providing users with secure and widespread access to necessary business data and applications improves communication within the organisation.

Furthermore, businesses can improve productivity by significantly reducing the time spent on password administration and maintenance by both users and help desk personnel.

The solution also helps enterprises comply with regulations by enabling secure user access and providing a proven method for protecting internal data and networks. This is important as an ever growing list of regulations, including Electronic Signatures in Global and National Commerce (E-SIGN) Act, Sarbanes-Oxley (SOX) Act, Basel II mandate that organisations protect their data and meet IT security standards.

Summary

In today's business environment, the weakness of passwords should no longer be tolerated. Organisations need to make the move from password-centric authentication to multi-factor authentication.

We at Unisys can provide the required expertise to protect online identities and business interactions with clients and customers - a strong and reliable authentication solution that reduces security vulnerabilities, helps you comply with regulations and enables more business by attracting security-conscious customers.

Expertise

Unisys security solutions can be found worldwide in 600+ airports, 1,500 government agencies, 100+ banks, among others. We focus on large-scale security initiatives, such as national-level identification systems, that require complex security system integration solutions across people, data, systems and physical assets.

For more information, contact your Unisys sales representative or visit www.unisys.com