BLACK BOX®
NETWORK SERVICES

UareU
Biometric Authentication Solution

Key Features

- State-of-the-art biometric security
- Elimination of logon and application passwords
- Reduced support costs
- Instant access with the touch of a finger
- UareU Sensor or UareU Fingerprint Keyboard
- Growth path that supports individual, departmental and enterprise-wide deployments

User authentication and authorization processes are the gatekeepers to your business systems, connecting users to the broader security infrastructure. Problems with the user authentication process can compromise the security of your business systems. The best designed system and application security is of little use if an authorized user gives their password to someone over the phone.

User authentication is proving problematic and costly for many organizations. The situation is analogous to the networking world, in which the "last mile" that connects users to a high-speed infrastructure can be the most difficult and costly to implement.

Until we can better handle the last mile of the security infrastructure, the entire infrastructure is at risk. According to the Computer Emergency Response Team (CERT), compromised passwords are involved with 80% of the security problems they investigate.

There is a better way to handle user authentication. Biometric technologies identify individuals based on their physical characteristics. The technology has matured in recent years, and is now ready for mass adoption. Fingerprint biometrics are a viable and practical alternative for user authentication, even for small and mid-sized organizations. BLACK BOX offers complete biometric authentication solutions – reducing the cost and risks associated with password authentication. Applications range from personal computing to corporate networks to web-based services:

UareU Pro
A complete, plug and play solution for biometric authentication in the corporate network, including networked administration tools for security administrators.

UareU Online
An Internet service that integrates fingerprint biometrics in e-signature security solutions for online services providers.
Available either as a hosted service or as server software.

Passwords: Imperfect and costly in practice
The traditional method for authenticating users is using passwords. The theory is simple; if a password is known only to a specific user, then someone providing that password must be who they claim to be. In practice, however, passwords are both insecure and costly.

Password security depends on individuals using them correctly. Research shows that people routinely fail to do so, making the same common errors:

- Setting passwords to predictable or easy strings. In an effort to remember their passwords, many people choose obvious or simple password strings. Password cracking software can automatically guess many passwords, particularly those set to whole words.
- Writing down passwords. To protect against password theft, companies often require "stronger" passwords with more special characters. These passwords prove more difficult to remember, so people sometimes

write them down – often at their workstations.
- Using the same password across many systems. People often set the same password on multiple systems – even frequently visited web sites. A hacker having discovered a password on one system is often able to gain access to many other systems.
- Giving away passwords. We should know better, but in a recent survey by security company PentaSafe, four out of five people would give their password to someone who worked in their company. Passwords are vulnerable to social engineering attacks.

In addition to the security issues, passwords create administration costs. The more frequently you make people change their passwords, the more likely they are to forget them. According to industry analysts, forgotten passwords can account for between 20 and 50% of a typical company's Help Desk calls. The higher range probably represents organizations with stronger password requirements.
More significant, but harder to predict, are the losses that could be prevented with fingerprint authorization. These include:

- Loss due to embezzlement or fraud. With security breaches on the rise, the risk of this loss increases annually. These actions can result either in direct losses or increased insurance premiums.
- Loss due to outage from a malicious attack. The direct cost of downtime depends on a business. Web site downtime can cost $50,000 per hour for an average retailer, and millions per hour for large financial institutions. (Source: the Meta Group)
- Loss due to data on stolen laptops. Some laptop thieves work airports and ransom the data on laptop hard disks back to the company or its competitors.

Improving security with fingerprint biometrics
Biometrics use physical attributes to confirm an individual's identity. Fingerprints are a tested and proven method for authentication, and can be implemented using relatively low cost sensors.
Fingerprint biometrics eliminate many of the security problems associated with passwords.

- People cannot forget their fingerprints, so there is no need to write them down or call a Help Desk for a reset.
- Fingerprints cannot be "guessed" by an outside hacker. There are simply too many possible variations. Although it is theoretically possible to lift someone's latent prints and fool the scanner, it is in practice difficult to do, and requir es a sophisticated attacker in close proximity to authorized users.
- Fingerprints are less vulnerable to social engineering attacks. No hacker can easily call someone else and ask for a fingerprint over the phone. It is difficult to "tell" someone else your fingerprint – you would have to actually put your finger on a sensor to give an unauthorized person access.

The savings in Help Desk calls alone can easily offset the hardware costs of the fingerprint scanners. (See the cost analysis section that follows.) More importantly, biometric authentication makes you less vulnerable to significant losses from security breaches.

UareU Pro biometric authentication system
Although fingerprints have been in regular use for a century as a means of identification in law enforcement, the use of fingerprints in a networked computer infrastructure is much more recent. Fingerprint sensors that work well in a controlled law enforcement climate do not necessarily meet the needs of users authenticating over insecure networks. The BLACK BOX UareU biometric authentication system is designed specifically to handle the needs of networked user authentication, addressing the security, privacy, usability, and cost concerns of this environment.
End-to-end security and privacy. Unlike other fingerprint solutions, the UareU sensor never sends unencrypted data, even between the sensor and the computer to which it is locally attached. All communication between the sensor and a trusted authentication server takes place on an encrypted, challenge/response link, so data cannot be intercepted and examined or re-used. In addition, fingerprint information is always private. The product never sends or stores a fingerprint image; the UareU templates cannot be used to recreate a fingerprint image.

Convenience and usability. The UareU fingerprint sensors are simple and convenient to operate. They can read prints from individuals young and old, in less than perfect conditions, with fingers placed at varying angles on the sensor. Setting up the system to identify your fingerprint is a simple process.
Flexibility. The BLACK BOX products integrate easily into different computing environments, whether you are installing on a Windows XP workstation or creating fingerprint authorization for online services.
Cost-effectiveness. Despite the small hardware investment involved in fingerprint scanners, the UareU biometric systems save you money relative to password authentication. The following section outlines cost savings for a sample organization.

Ordering information

ITEM	CODE
UareU Pro Standalone Workstation with Fingerprint Sensor	83111-001
UareU Pro Standalone Workstation with Fingerprint Keyboard	83130-001
UareU ro Starter kit for 10 Workstations	83001-001
UareU Pro Server Software	63000-001
UareU Pro Server Single User Access License	93001-001
UareU online	on request