Uncompromised Two Factor Authentication Using BiObex's Strong Authentication Front End (SAFE) Technology

Overview

BiObex's SAFE (Strong Authentication Front End) Technology implements a patented digitally signed two-factor authentication and provides three distinct operational capabilities: login, file protection, and digital signature all with a single device. BiObex has filed several patents related to SAFE Technology: Five (5) patents awarded and three (3) pending.

The SAFE-Key device has undergone the rigorous government testing of FIPS 140-2 Level 3 Certification. The SAFE-Key device will be the ONLY device of its kind that has Level 3 status. The expected date for Certification submission is May 2017.

One SAFE-Key – Multiple Capabilities

1 Digitally Signed 2FA

- Familiar User Experience
- Web-based and Desktop Login

2 Digital Signature

- Validates the Sender
- Verifies Document integrity

3 SAFE Protected Files (SPF)

- Encrypt and Store Files
- Encrypt, Digitally Sign, & Send, Files & Email

Digitally Signed – Two-Factor Password Authentication

SAFE-Key Login maintains the simple username and password user experience while providing cryptographically verified and protected two-factor authentication. When the user authenticates (using their password), hacking attempts such as phishing, keylogging, man-in-the-middle, man-in-the-browser, and replay are defeated. A challenge-response protocol prevents the login packet from being hijacked or replayed. The SAFE-Key password protocol combines both factors: "something you have" and ("something you know", i.e. the device ID and i.e. the user's password), as well as a challenge response, into a single password packet that is encrypted and digitally signed. The authentication evidence is thus intertwined and cannot be separated in transit. The challenge response ties the packet to a particular authentication session, which prevents it from being replayed or hijacked for a different authentication session. The encryption protects the evidence from discovery and reuse. The digital signature provides a strong cryptographic means of verify the device ID that is robust against hacking attacks such as database breaches.

SAFE-Key Login technology requires complimentary software on a server. The SAML protocol can be used to connect this authentication service to any authorization point. A single SAFE-Key Login server supports multiple independently administered login domains.

Digital Document Signatures

A SAFE-Key device can be used to cryptographically sign a document. The signature can only be generated using the SAFE-Key device's device-specific private key, but the origin and validity of the document can be confirmed by anyone with knowledge of the SAFE-Key device's public key. The SAFE-Key device enforces two-factor authentication by requiring password verification before generating the signature.

SAFE Protected Files (SPF)

A SAFE Protected File ensures that only the intended recipient can decrypt the file. The file is encrypted by a software-only package using the SAFE-Key device's public key. Only the selected SAFE-Key device, with its device-specific private key, can then decrypt the document. The device enforces two-factor authentication by requiring password verification before decrypting the document. All data is protected at rest and in transit.

©2017 BiObex, LLC All Rights Reserved. BiObex and SAFE are registered trademarks.