LoginShield

Our mission: empower organizations to eliminate the threat of password and phishing attacks on their users

OVERVIEW

One-tap login is the most convenient way to login to a website or application

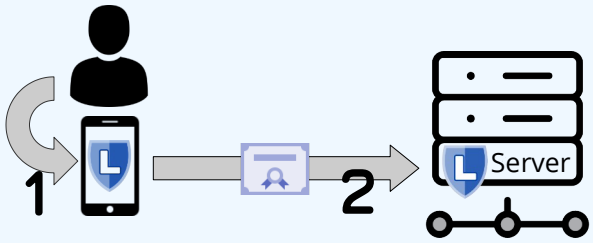
Strong multi-factor authentication with digital signatures eliminates costs & risks associated with password authentication, including stolen passwords, weak passwords, reused passwords, and shared passwords

A unique patent-pending system protects users and assets against phishing attacks

MULTI-FACTOR AUTHENTICATION

1. Unlock app with passcode or fingerprint

2. Authenticate with digital signature



FEATURES

Unique asymmetric key generated for each account

Encrypted key backup not readable to service operator

When device is lost or damaged, recover from backup with identity verification, secret recovery codes, and geolocation

Automatic key synchronization among multiple devices

When device is lost, stolen, or compromised, disable all authentication from device so any extracted private keys cannot be used in authentication

Authenticator routes around untrusted sites so user always arrives at intended website

CRYPTOGRAPHY

Device storage master key derived from passcode using PBKDF2 with SHA-256

Encryption key and integrity key derived from master key using HKDF with SHA-256

Private keys encrypted on device with AES-128 and data integrity check with HMAC-SHA256

Authentication using RSA 2048-bit keys with SSA-PSS, SHA-256, MGF1

Communication between system components protected using TLS 1.2 or higher with common cipher suites

Communication passing through untrusted external components protected using AES-GCM with 128-bit data encryption key

Data encryption key distribution protected using RSA 2048-bit keys with OAEP, SHA-256, MGF1