Biometric Signature ID

Corporate Background Technologies, Capabilities, and Products FedGov/DoD 2023

biosig-id.com

America's most valuable and sensitive national defense assets and information, are managed and protected leveraging secure digital telecommunication networks.

We are in a new "cold war", and our adversaries constantly try to illegally gain access to these networks by falsifying the stolen or compromised digital identity and credentials of lawful operators.

Our adversaries' aim is to disrupt our national defense apparatus, and put our national security at risk.

Biometric Signature ID (BSI) is a biometrics cyber security company with patented technologies and solutions to protect access to sensitive information. We create and manage secure biometric online access credentials that are PII free, and are impossible to replicate by enemy or machine.

We protect the warfighter online and real world identity through Complex Multi-Factor Authentication (CMFA) in a simple and reliable authorized user experience.

We are 100% compliant with biometric privacy laws, and link online digital access to the authority of the cleared warfighter's presence; not their credentials.

Fight your adversaries; we'll challenge anyone even near your digital post, and will allow no one to pass without the proper authority.

About BSI

J.C. Lads Corporation is doing business as "Biometric Signature ID" (BSI) since 2007. It is a Small Business Texas "C" Corporation, headquartered in Lewisville, TX.

BSI has been called upon to collaborate with other leaders in the White House's NSTIC selected biometric technology forum, and was invited to join NASPO as committee member.

BSI was recognized as a Top 20 Ed-Tech company, and its technology has been featured in no less than 20 trade journals.

A different type of biometrics...

...for a new cold war.

Our adversaries continuously evolve their cyber capabilities and tactics, trying to keep ahead of our national security apparatus.

Through complex artificial intelligence (AI) and machine learning (ML) algorithms, they reproduce and continue to successfully steal even the most complex Multi Factor Authentication (MFA) methodologies and physically bound biometric credentials.

BSI is redefining MFA and Biometrics, going around the current threat and delivering a form of online credential that is:

1. **Behaviorally linked to, and is successfully reproduced by only one person in the world; the one who created it.**
2. **Irreplicable by any other human, AI, or ML algorithm; and thus not worth the effort, and attention of a cyber criminal.**

Patented and in commercial use.

BSI owns two active US technology patents with 44 claims for the use of behavioral biometrics that are 100% free of PII.

Both patents focus on storing and analyzing continuous vector lines (CVLs), which are the core elements of BSI's products and solution.

BSI's underlying technology analyzes the way in which human users use touchpads, mice, stylus, or their fingers to implement hand-written passwords that can't be falsified.

No special or additional hardware required - it just works.

2 Patents
44 Claims
0 PII

232+
Clients

2M+
Users

100M+
Authentications with less than 0.045% help desk calls

COTS Solutions Family at TRL 7-9

A patented biometric identity authentication solution that controls access to files and information through MFA in one product. It works on all devices using HTML5.

- Requires no hardware or software downloads and authenticates users with a four-character password.
- Blends amazing biometric technology with the password format users are comfortable with.
- Provides real-time warning of potential data crimes in progress.

BioSig-ID™

Applications:

- Any time “attribution” of action is needed
- SCIF credential validation / log in & out
- Computer session management
- Code programming version control attribution
- Sensitive records access and control

Prevents unauthorized access to Windows workstations, tablets, laptops, and the information and files within, by replacing the device’s native lock screen.

- Grants access to devices after a successful authentication.
- Identity credentials can be stored locally, to allow temporary use offline.
- Protects workstations and blocks access to unauthorize users like RDP attacks.
- Allows administrators to monitor and change device acces aability, reset passwords, and audit illicit access attempts.

BioTect-ID™

Applications:

- Any time “attribution” for access is needed
- Access to cryptographic equipment
- Use of “High Side” computer equipment
- CAC augmentation

Used for the initial ID verification of an individual.

- Analyzes the person’s government issued documents and checks the front and back to determine legitimacy of the OCR codes.
- Stores a user approved “selfie” of the user, used to compare with photo in the government ID.
- Provides both, verification AND authentication of identity.

BioProof-ID™

Applications:

- Any time “attribution” for access is needed
- CAC registration / validation
- Chain of custody material exchange

BioSight-ID™

Applications:

- TRADOC CBIT
- Promotion exams for enlisted personnel
- eLearning for any MOS school
- “High Side” VTC management

Used for automatic proctoring of online training and continued education programs.

- Does not collect any biometric markers and protects the privacy of the user by blurring all images
- Works seamlessly with the world’s leading learning management systems (LMSs)
- Provides complete class and course analytics and guides instructors to find suspicious activity by the student.

BioName-ID™

Applications:

- Remote digital order execution / signature
- Supply chain management SF1250 use
- Watchstander logs for weapons and critical systems.
- Maintenance record certifications
- Quality assurance chain of custory management

Transforms signatures into digital identity.

- Prevents use of PNG/JPEG forgeries
- Eliminates the need for “wet ink” to attribute the signature to a human.
- Authenticates signatures through tamper-proof MFA in a single application.

BioSafe-ID™

Applications:

- Supply chain management
- Government “impact card use” validation
- SCIF / Sensitive documentation management

Secures online transactions.

- Prevents “card not present” fraud
- Ensures that the transaction is executed by the human owns the credit card, not the “entity” that may have the digital credentials.