AUTHENTISE SECURE

Security and intellectual property protection for Additive Manufacturing

August 2015

AUTHENTISE

www.authentise.com | secure@authentise.com

Our additive manufacturing security tools enable direct-to-machine design transfer. Ensure design and machine integrity, pervasive action monitoring and protect revenue and intellectual property. Authority to print and business rules can be centrally administered and updated, the service is available as an API and hosted version. Use our technology to:

- Start distributing products digitally
- Protect integrity of designs during co-creation process
- Secure your supply chain
- Protect yourself against regulation (DFARS)
- Enable in process quality assurance
- Provide supply chain visibility
- Report accurate historic data to forecast costs
- Deliver real time on-demand production near point of use

Features

Secure Access

- Multiple delivery options: Streaming, Hosted, Local, Encrypted file delivery
- Always with the highest protection: Secure communication via TLS v1.2, Strong encryption via AES-256 block cipher

Access Control

- Business Rules Logic: Different access level for different use cases
  - Devices: Access to an specific machine
  - Locations: Access to machines in an specific location
  - People: Access based on identity.
- Monetization: Define your own monetization strategy
  - Pay-per-print
  - Subscription
  - Life-time access.

Design Integrity

- Parameter lock: Make sure all prints are performed using the same parameters and on a limited range of machines.
- Open only a few of the parameters: Allow machine operators or other stakeholders to tweak a specific subset of parameters.

- Material lock: restrict prints to certain materials
- Provenance test to identify whether file was handled correctly in its life cycle*

Tracking through Advanced Watermarking

- One file instance per print: We always generate a new file for every new print
- Guardtime: The joint solution offers design owners the ability to trace their data in any circumstance*
- Watermarking File: Hidden copyright notices or other verification messages in the design file or machine code*
- Steganography: Insertion of hidden references in the physical product authenticating or warning of the product's origins.*

Quality Assurance:

- Through Monitor: Market-leading options for two core quality assurance needs: melt pool monitoring and detection of defects in the powder bed during layer preparation.
- Through Feedback: Use machine logs and feedback data to check print quality.

Extensible

- Through 3Diax data security can secure the entire digital thread, from design to production, including quality monitoring.
- Working with Siemens on extending security application to CNC and other digitial manufacturing tools*

Delivery Mechanisms

The printer instructions are transmitted within a secure tunnel. This tunnel uses a 256 AES block cipher after negotiating an ephemeral Diffie-Helman key exchange.

Streaming

Production instructions are kept in a small in-memory buffer close to the controllers of the printer. This buffer keeps only a few minutes of instructions at any given time reducing the attack surface and requiring a persistent connection for ongoing security.

Hosted

Authentise Secure operates servers with industry standard cloud security. Backend processing servers are maintained in a separate subnet from front-end web request handlers with gateway machines controlling access between the servers. Data storage is kept in a third secure area. Each area can scale with load and includes redundancy in case of failure. Customers can self-encrypt or use our hosted encryption keys. All transactions occur over SSL

Local*

Authentise Secure instances can also be deployed within your perimeter or hosted on your servers to supply you network. If necessary, our engineers will assist you to deploy the solutions on AWS GovCloud or your own OpenStack deployment.

Encrypted File Delivery

If desired, the in-memory buffer on the device can be expanded to 100% of the file size on the fly. The in-memory buffer remains protected and the encryption on delivered data is not released until immediately prior to the production process

Contact

To discuss licensing options and partnerships: secure@authentise.com

The publicly available consumer version of Authentise Secure is available through 3Diax.

** While all our features are under constant development, the features marked with an asterisk have not yet been deployed publicly*