BCD Asset Engine Workspace
DWS
Powered by Dynamic Workflow Solutions

SOLUTION OVERVIEW

AUTHENTICATION powered by Swear™

Independent blockchain authentication, built into the workflow

Independent proof, built into the engine

SWEAR is the authentication component of the BCD Digital Asset Engine (DAE). From ingest on the Field Intelligence System (FIS) to disclosure and court, it anchors proof-of-original on an independent blockchain ledger, while Hybrid 5.0 keeps the media in the agency's own on-premises and cloud storage.

2 of 8 stages
Authenticate and Re-Authenticate in the DAE workflow

Independent
ledger, separate from the DAE and agency storage

Hashes only
the media never leaves agency storage

Frame by frame
validation against the ledger

THE CHALLENGE

Seeing is no longer believing
Deepfakes and synthetic media are eroding confidence in recordings across law enforcement and the courts.

Self-attested proof is not enough
A hash kept in the same system as the file only proves what that system says.

THE DIGITAL ASSET ENGINE WORKFLOW

1 — Ingest on the Field Intelligence System
DAE hashes content and logs chain of custody (COC) at intake.
DataCentral Digital Asset Engine

→

2 — SWEAR — AI Authentication
SWEAR applies blockchain-anchored proof-of-original for deepfake protection.
Authenticate

→

3 — Convert to MP4
Proprietary video from any source is normalized into a standard container.
Normalize

→

4 — SWEAR — Re-run Authentication
SWEAR re-anchors after conversion, so proof-of-original stays unbroken.
Re-Authenticate

↓

5 — BriefCam Video Search (optional)
Video analytics for search and review on GPU FIS or Workspace tiers.
GPU Enabled VSS

←

6 — Secure Redaction
AI redaction of faces, plates, and identifying detail.
Redaction

←

7 — VALIDATE — Clip Editor
Trim and export clips of interest from verified footage on the spot.
Rapid Clip Distribution

←

8 — VALIDATE — Map Evidence to DEMS / DAMS or Archive
Triage and share from the field via DataCentral to the DEMS of choice.
Build the Investigative File

■ SWEAR authenticates and anchors to the independent ledger
□ SWEAR validates verified footage before it is shared or filed

SWEAR TOUCHPOINTS

1 — Capture
Camera, VMS, and Field Interview Kit (FIK) media certified at the source.

2 — Ingest
FIS or Workspace authenticates on intake.

3 — Chain of custody
Re-anchored after the MP4 rewrap.

4 — Storage
Hybrid 5.0 holds media; the ledger holds proof.

5 — Disclosure and court
Every frame checked before release.

BCD Asset Engine Workspace

DWS
Powered by Dynamic Workflow Solutions

SOLUTION OVERVIEW

AUTHENTICATION powered by Swear™

Independent ledger, Hybrid 5.0 storage

Your storage. Independent proof.

Hybrid 5.0 Cemented e-DAMS is BCD's fifth-generation architecture for running enterprise digital asset management across on-premises and cloud environments at once. It binds FIS, Workspace, and Archival Services into one governed system, so an asset behaves the same way wherever it is stored. SWEAR adds the one thing an agency's own system cannot supply: proof of authenticity held outside it.

TWO PLANES, ONE RECORD

AGENCY CONTROLLED

Hybrid 5.0 Cemented e-DAMS

FIS | Workspace | Archival Services

- Originals, MP4 conversions, redactions, and clips
- Audit logging of every view, share, edit, and approval
- On-premises, private, public, or hybrid cloud storage

→ Hashes and timestamps only

← Validation results

INDEPENDENT

SWEAR ledger

Ingest API | Ledger of hashes | Search API

- Fingerprints, timestamps, and opaque transaction identifiers
- Mapped to a tamper-evident blockchain network
- X.509 identity with strict permissioned participation

SWEAR ACROSS THE ENGINE

Touchpoint	DAE and Hybrid 5.0 component	SWEAR contribution
Capture	Cameras, body cameras, VMS, and FIK	Certification during recording through SWEAR's capture integrations.
Field ingest	FIS rugged laptop, stages 1 and 2	Authenticates at intake, beside the DAE hash and COC log.
HQ ingest	DAE Workspace, stages 1 to 4	Authenticates on ingest and re-authenticates after MP4 conversion.
Derivatives	Redaction and Clip Editor, stages 6 and 7	Clips and redactions are cut from footage already verified.
Storage	Archival Services, Hybrid 5.0 storage	Media tiers on-premises or in the cloud; proof stays on the ledger.
Disclosure	Share links and DEMS publication, stage 8	SWEAR Validation for court, standalone or in playback, frame by frame.

WHERE IT FITS IN THE BCD ISG ARCHITECTURE

LAYER 01
Edge Hardware

- FIS field kit
- Rugged laptop and GB10
- Field Interview Kit (FIK)
- Digital Asset Workstation

LAYER 02
Orchestration

- Digital Asset Engine
- Hybrid 5.0 e-DAMS
- Data Central Evidence Engine
- **Authentication** SWEAR

LAYER 03
AI-Driven Processing

- Redaction
- Transcription
- Translation
- Visual search, agentic AI

LAYER 04
Storage and Retention

- On-premises Dell
- Hot cloud object
- Tiered cloud
- Offline, long-term

Intelligently managed end to end by the Digital Asset Engine and Hybrid 5.0

BCD
Asset Engine Workspace
DWS
Powered by Dynamic Workflow Solutions

SOLUTION OVERVIEW

AUTHENTICATION powered by Swear™

For the evidence management community

WHAT SWEAR ADDS TO THE ENGINE

Point-of-creation certification
Where integrated at the source, authenticity is mapped during recording, not after.

Forensic-grade validation
Fingerprints are recomputed during review and compared with the originals on the ledger.

Multi-channel Digital DNA
Frames, audio, and metadata are fingerprinted, so splicing, dubbing, or metadata tampering is detectable.

AI-resistant evidence
Verified originals can be distinguished from AI-generated, synthetic, or manipulated media.

WHY AN INDEPENDENT LEDGER MATTERS

Independent of storage
Proof does not depend on the system holding the file.

Tamper-evident record
A distributed, blockchain-backed, independently verifiable ledger.

Independent of the owner
A court need not take the agency's word for it.

Media stays home
Only hashes and timestamps are stored remotely.

WHY BCD ISG

- **Built into the workflow:** stages 2 and 4 of the DAE.
- **Independent by design:** proof lives apart from your systems.
- **Hybrid by default:** media stays in Hybrid 5.0 storage.
- **Unbroken after conversion:** re-anchored on rewrap.
- **Edge to courtroom:** FIS, FIK, and Workspace in one record.
- **No rip-and-replace:** works with existing cameras and VMS.

WHO IT'S FOR

Detectives and investigators · Prosecutors and DAs · Courts · Real-Time Crime Centers · Auditors and compliance · IT and evidence technicians

WORKS WITH

Dell · NVIDIA · Dynamic Workflow Solutions · BriefCam · BCD FIS · Hybrid 5.0

alongside body cameras, smartphones, and any VMS stream.

GETTING STARTED

1. **Discovery**
Where could authenticity be challenged, and where do your hashes live today?

2. **Proof of value**
Run sample footage through the DAE, alter a copy, and watch validation flag it.

3. **Design**
BCD places SWEAR at the source, in FIS, or in Workspace.

4. **Deploy and train**
BCD integrates validation into review and trains evidence staff.

- **Prove it is real**
Evidence you can prove, defend, and trust.
- **Stand apart**
Proof that does not rely on your systems.
- **Counter deepfakes**
Verified originals stand out from synthetic media.

SWEAR and the SWEAR Authenticity Platform are products of SWEAR. BCD FIS, the Digital Asset Engine Workspace, and Hybrid 5.0 are powered by Dynamic Workflow Solutions. Dell is a trademark of Dell Inc. NVIDIA is a trademark of NVIDIA Corporation. BriefCam is a trademark of BriefCam Ltd. All other trademarks are the property of their respective owners. Capabilities vary by integration and configuration. Copyright © 2026 BCD. All rights reserved.