

Protecting the Official Record in the Age of AI Manipulation

April 15, 2025

The treat isn't if recordings are manipulated, - it's proving they weren't. Digital signatures give courts a secure, verifiable chain of custody.



As artificial intelligence (AI) tools like deepfakes and voice cloning become increasingly realistic and accessible, **courts and law enforcement agencies alike** face new challenges in maintaining the integrity of digital evidence.

The question is no longer *if* recordings might be manipulated—it's *how courts and agencies can prove that they haven't been*.

While no one can fully control what happens to a file once it enters the public domain, both **judicial bodies** and **law enforcement departments** can take strong measures to protect the authenticity of recordings while they're still under official custody. One of the most effective ways to do this is through **digital signatures**, which provide cryptographic proof that a recording has not been altered since its creation.

The Real-World Threat: Quiet Tampering, Not Public Disinformation

While much of the public discourse around AI manipulation focuses on viral deepfakes or misinformation, the greater risk to the justice system lies in **subtle, behind-the-scenes tampering**. The most dangerous actors aren't posting content online—they're quietly attempting to:

- Undermine a ruling or verdict
- Remove or obscure evidence
- Introduce falsified media in post-trial motions
- Alter notes or metadata to mislead record interpretation

Protecting the record starts with controlling access. Recording systems—whether they’re capturing a courtroom hearing or a custodial interview—must enforce role-based access controls to ensure that only authorized personnel can initiate, manage, or retrieve recordings. This foundational layer of security significantly reduces the opportunity for tampering by limiting who can interact with sensitive files.

And even though [Liberty also supports RBAC through tools like Liberty Web Access](#), access control alone isn’t enough.

Even in tightly secured environments, courts and agencies must be able to **prove** that a file is authentic and unmodified—and that’s where digital signatures play a critical role.



What Is a Digital Signature—and Why Does It Matter?

A **digital signature** acts like a tamper-evident seal for a digital file. Think of it as the modern equivalent of sealing an envelope with wax: it confirms the contents are untouched and flags if anything has been changed.

When a recording is finalized in **Liberty Court Recorder** or **Liberty Interview Recorder**, the software can automatically apply a unique cryptographic signature that captures two key elements:

1. The exact date and time the file was completed
2. A mathematical fingerprint of the file’s contents

If the file is edited—even subtly—this fingerprint no longer matches, and the signature verification fails.

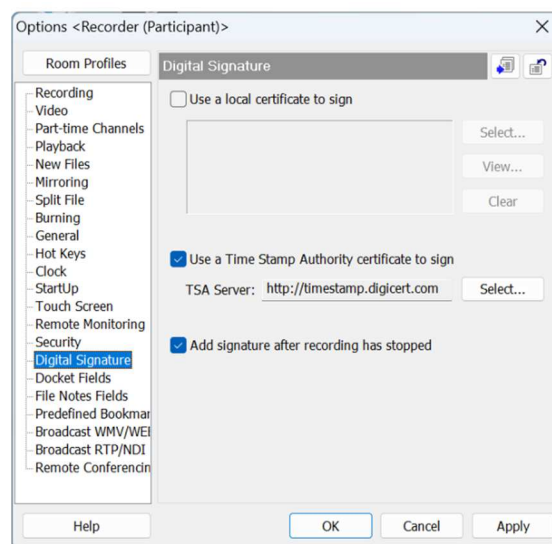
Unlike basic file properties (like "last modified" timestamps), **digital signatures are cryptographically verifiable, resistant to spoofing, and legally admissible as proof of integrity.**

This creates a tamper-evident **chain of custody**—ensuring that official recordings remain authentic, complete, and defensible in any proceeding or investigation.

How to Enable Digital Signing in Liberty Court Recorder or Interview Recorder

If your court or agency is running the latest version of Liberty Court Recorder or Interview Recorder, enabling digital signatures is simple:

1. Go to File > Options > Digital Signature
2. Choose your signing method:
 - Use a **local certificate** (provided by your IT department), or
 - Select a trusted **Time Stamp Authority (TSA)** such as DigiCert or GlobalSign
3. (Recommended) Check the option for **“Add signature after recording has stopped.”**
 - This ensures each session is automatically signed when it ends—avoiding manual steps.



To sign a completed recording manually:

- Go to File > Sign in either program.

This applies a trusted digital seal to the file, locking it in its original state and making any future tampering detectable.

Verifying a Recording for Tampering

If a recording's authenticity is ever questioned—whether during a trial, a review board hearing, or a criminal investigation—staff can use **Liberty Court Recorder**, **Interview Recorder**, or the **Liberty Player** to verify the digital signature:






- Open the file
- Select File > Verify Signature

If the file has been altered since it was signed, the system will clearly indicate that the signature is invalid. If the file is intact, the software will confirm that the **signature is trusted** and **the data has not been modified**.

While the system won't pinpoint the exact change, it will identify the type of modification (e.g., media, bookmarks, notes, metadata)—providing helpful insight during the review process.

Recommended Best Practices for Courts and Law Enforcement

To strengthen your approach to recording integrity:

-  **Enforce role-based access controls** within the recording system
-  **Digitally sign recordings** at the end of each session using secure certificates
-  **Train judicial and investigative staff** on how digital verification works
-  **Retain only signed originals** in secure, centralized storage
-  **Avoid circulating unsigned copies**, especially in high-profile or sensitive cases

These practices don't just protect your evidence—they help build trust with the public, the press, and the legal system as a whole.

Final Thought: A Trusted Record in a Changing World

In a digital environment where AI-generated content is reshaping perceptions of truth, the **integrity of the official record is non-negotiable**.

By combining secure access controls with cryptographically verifiable digital signatures, courts and law enforcement agencies can ensure their recordings are tamper-evident, trustworthy, and future-proof—no matter what challenges lie ahead.

If your organization is ready to implement digital signing—or if you'd like help reviewing your current recording security practices—contact Liberty Recording at: support@LibertyRecording.com.