Digital Signatures & the Future of Trust in Construction

CONCERT

Introduction

For over a century, the seal and signature of an architect or engineer have carried significant weight. A stamped sheet, wet-signed in ink, is not just a mark — it is a declaration of responsibility for the health, welfare, and safety of a building, bridge, or other works of infrastructure. Trust itself is embodied in that mark.

As digital technologies have become mainstream, the AEC industry has pivoted from inked sheets to electronically signed PDFs, with only a handful of jurisdictions still requiring wet seals. But those signatures remain tied to the old form: a sheet with an area in the title block for a seal. This pivot was smooth because it merely digitized the familiar signature block.

But a signature on a set of PDFs is no longer sufficient to capture accountability for the full range of digital work products for two principal reasons:

1. The scope of data driving project execution has **expanded dramatically.**

2. We now work in digital environments that are **not intended to be printed.**

What follows is a more challenging transition as the AEC industry moves beyond documents toward data-driven deliverables, yet our system of trust has not kept pace. Before exploring the full dimensions of that gap, it is worth pausing here – the signature has always carried the weight of responsibility, but how should that responsibility be expressed when the work product no longer has a paper analog?

The Problem

Construction has gone digital, but the trust system behind it has not. What we have today is **extremely limited**. It works for a narrow band of situations and leaves most real project data uncovered.

Single format. In practice, the system works only with PDFs. Teams exchange data in various forms, including CSVs, schedules, models, code, and video. None of that is supported.

"The industry delivers in many formats, but only PDFs get protection."

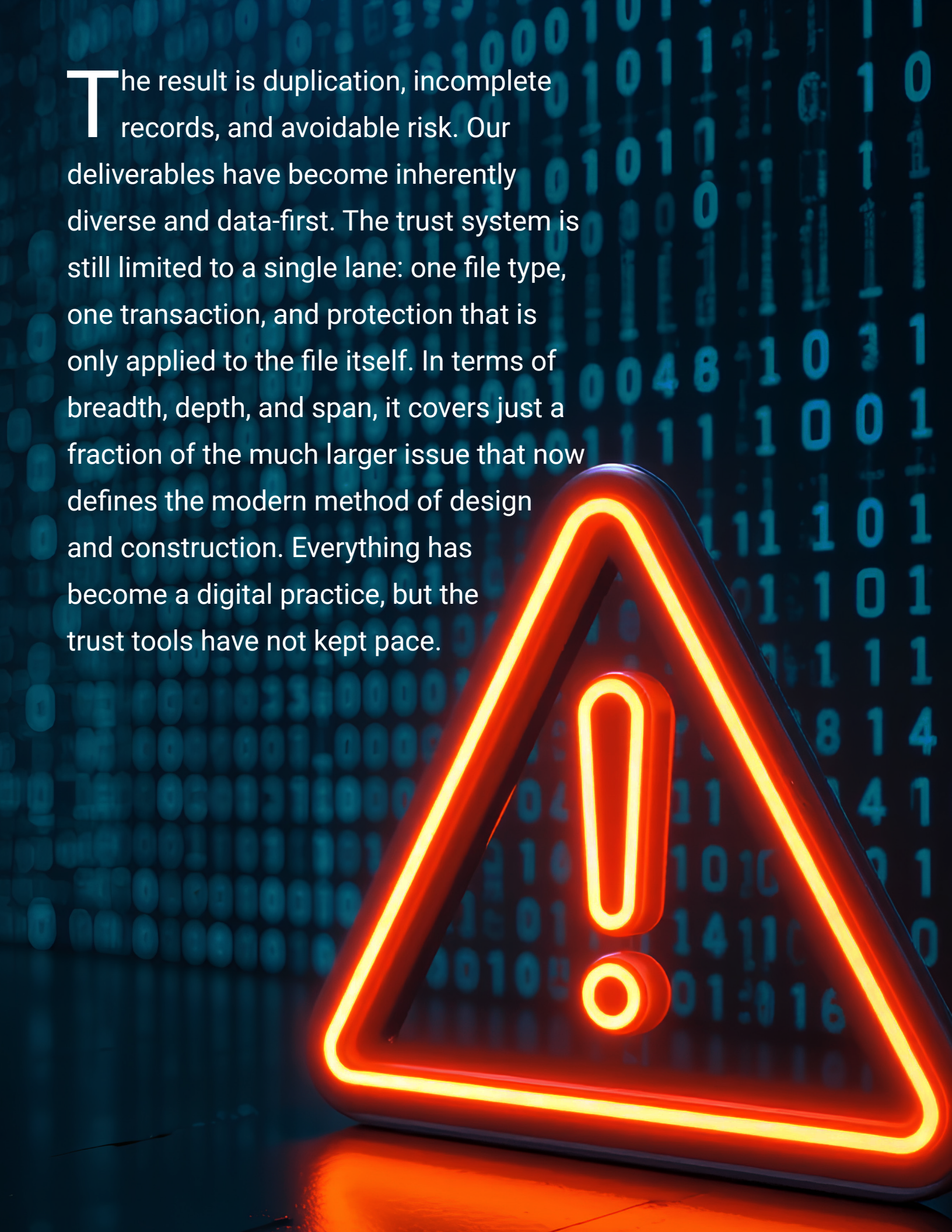
Shallow protection. A signed PDF can prove that the file hasn't changed since it was signed. It cannot prove who signed, whether that person was licensed, or what act of authorization the signature represents.

"Today's PDF protects the artifact, not the author or the authorization."

Narrow deliverable scope. The current system covers stamped Construction Documents for permitting. But projects span a much longer period from pre-design through handover, and in the future, may even extend to operations.

"Most of what moves a project forward sits outside the trust system."

The result is duplication, incomplete records, and avoidable risk. Our deliverables have become inherently diverse and data-first. The trust system is still limited to a single lane: one file type, one transaction, and protection that is only applied to the file itself. In terms of breadth, depth, and span, it covers just a fraction of the much larger issue that now defines the modern method of design and construction. Everything has become a digital practice, but the trust tools have not kept pace.



The Solution

To move forward, the trust system must match how projects actually work:

Breadth of Formats. Apply not only to PDFs but to drawings, spreadsheets, models, schedules, datasets, CNC instructions, and even video or robotics.

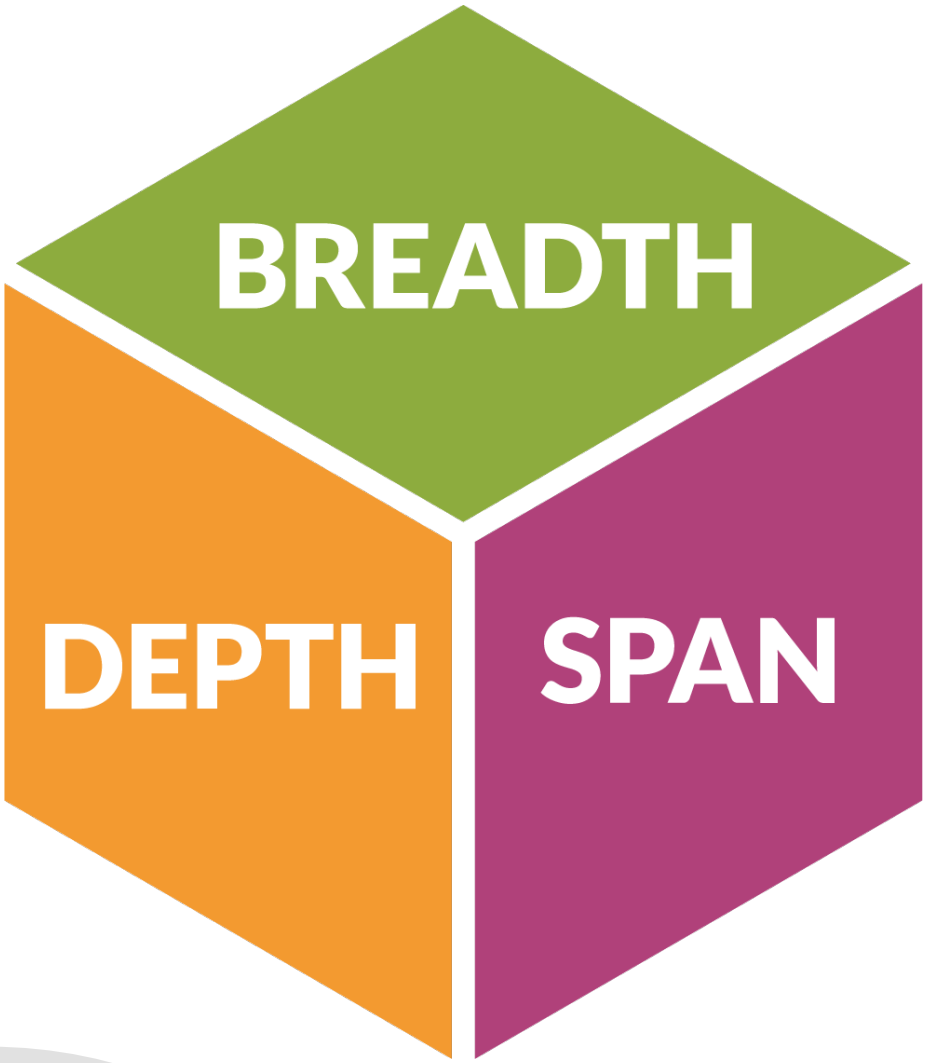
"From one format → to every format a project produces."

Depth of Protection. Confirm who signed, whether they were authorized to do so, and preserve that act permanently.

"From file-only protection → to protecting the author and their authority."

Span of the Project Lifecycle. Extend across the entire project, including construction documents, RFIs, directives, memos, and owner communications.

"From one deliverable → to the whole life of the project."



This is what it means to expand trust. Trust becomes three-dimensional — deep enough, broad enough, and expansive enough to hold the way projects are delivered today. And because it works at the level of digital fingerprints, not document shapes, it is also ready for what comes next: new formats, new workflows, even file types that haven't yet been imagined.

Why Now?

The industry has been promised a digital future for years. Revit came out almost 30 years ago. Since then, progress has come in fits and starts: the UK mandated BIM for public projects in 2016, the EU introduced BIM requirements for public works more recently, the U.S. GSA and Department of Defense issued BIM guidance, ISO 19650 established global standards for information management, and the 2021 Infrastructure Investment and Jobs Act allocated funding tied to digital delivery. AIA's contract form e203 (2022) made clear that models and data could stand as instruments of service. The U.S. Department of Transportation's Model as the Legal Document (MALD) initiative now signals that the transportation industry is preparing to transition to model-based delivery.

Yet BIM and model-based delivery alone are not the end of project execution. Teams still require visualization, itemization, and various other methods of viewing and working with project data beyond BIM itself. Despite all these signals, the firepower is still lacking. Without a trust system, the shift risks becoming a colossal flop.

CONCERT breaks through this barrier, making it possible to treat any deliverable — spreadsheet, model, dataset, or code — as an instrument of service affirmed by authority and authenticity.

With CONCERT, a bridge exists. For the first time, firms can work in both worlds at once:

- ☒ Submit PDFs with the identical signatures that regulators already accept.
- ☒ At the same time, secure models, datasets, and project communications in the very same system.

This is not an incremental change. It is an opportunity to establish a trust system that works now — across the depth, breadth, and span of today's deliverables — and will continue to work as new forms of data emerge.

That is a compelling event. The firms that adopt now will protect today's work and own the digital future. Those who wait will remain stuck in duplication, liability, and a trust system built only for PDFs.

A Brief History of Digital Signatures

UETA & ESIGN (1999–2000). These U.S. laws gave electronic signatures the same legal authority as physical ones. The Uniform Electronic Transactions Act (UETA) model law states that a signature, contract, or record may not be denied legal effect solely because it is electronic. The federal ESIGN Act reinforced the same principle nationwide. Without this recognition, digital methods of signing had no binding force, regardless of technical capability.

DSS (1994 onward). NIST's Digital Signature Standard defined cryptographic methods to secure digital artifacts. Most state codes echo its four criteria: (1) the signature must be unique to the signer; (2) it must be capable of verification; (3) it must be under the sole control of the signer; and (4) it must be linked to the data such that any change invalidates it. DSS only became practically relevant once UETA/ESIGN established that electronic documents could be legally signed.

PDFs as the Standard. The combination of DSS, UETA/ESIGN, and Certificate Authorities found its practical expression in the PDF format. Adobe's adoption of DSS, marked with a visible blue ribbon, made PDFs the de facto standard for digital signatures. Other document types never gained the same traction. In practice, DSS/CA signatures work by injecting metadata into the PDF — a hidden cryptographic layer that is not physically connected to the visible seal but is backed by a chain of trust. This injection made PDFs practical for regulators and users, but it also confined DSS to a document-centric model. Models, spreadsheets and code lacked consistent methods for embedding and presenting signature metadata, so DSS never naturally extended beyond PDFs.

Breadth of Formats

Today's trust system is effectively limited to PDFs. DSS signatures work there, and permitting authorities have shaped their digital portals around them. CONCERT provides that same DSS protection for PDFs, but it also adds blockchain memorialization to all file types, including PDFs themselves. The difference is critical: DSS injects a certificate into the PDF's metadata, while CONCERT takes the final intact version of any file, generates a digital fingerprint, and records it on a blockchain. This means every file can be authenticated without alteration, opening the door to trust across today's formats and those yet to be created.

CONCERT secures all of them. Projects run on many types of files:

- ☒ PDFs for permitting
- ☒ Drawings and BIM models
- ☒ Spreadsheets and schedules
- ☒ Datasets and analysis outputs
- ☒ CNC instructions and robotic code
- ☒ Video, AR/VR, and other visualization outputs

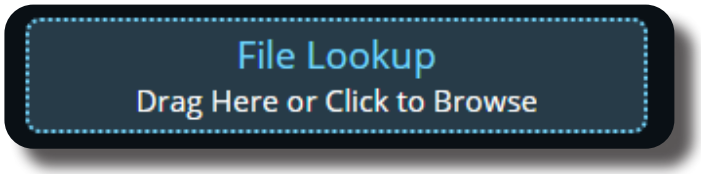
The contrast is simple:

- DSS protects PDFs.
- CONCERT protects files in any format, and makes each one independently verifiable.

How to Verify Authenticity, Authorship and Provenance

CONCERT enables three complementary ways to verify trust across formats:

File Checking Portal. Any participant can upload a file to CONCERT's portal and instantly check its fingerprint against the blockchain record. If the fingerprint matches, the file is authentic and current; if not, it has been altered or superseded.



Attestation of Authenticity. Each authorized file can be accompanied by a printable certificate that attests to its authenticity, authorship, and inclusion in a deliverable set. This creates a durable paper trail in conjunction with the digital record.

QR Codes on PDFs. Every printed PDF carries a QR code that expresses the date and currency of the deliverable. Scanning the code reveals whether the sheet is current, overwritten, or corrected. This feature is critical in the field: a sheet taped to a construction trailer wall may remain there for months or years. With the QR code, the carpenter, electrician, or inspector holding that sheet can confirm in seconds whether it still conforms to the project's original intent.

Together, these mechanisms ensure that authenticity, authorship, and provenance are preserved not just in principle, but in everyday practice.

Depth of Protection

For PDFs, CONCERT continues to support the CA-based system that regulators already recognize. But for everything else, CONCERT applies a separate regime that reflects the spirit of DSS without being bound by its limitations. Instead of injecting data into a file, CONCERT takes the file exactly as it is and generates a digital fingerprint (cryptographic hash). That fingerprint is then written into a public blockchain record. A single change — even a dot on a sheet — produces a different fingerprint, making tampering obvious.

CONCERT adds further protections not provided by DSS alone:

- ☒ **Verified identity.** Each signer is confirmed by multi-factor authentication and a one-time validation process that ensures the person is truly the designated signatory.
- ☒ **License validation.** Signatures are checked against active licenses, tying every authorization to professional authority. Expired or suspended licenses cannot be used to sign.
- ☒ **Immutable record.** Each act of authorization is written both to a certificate authority and to a public blockchain, providing a permanent, auditable trail.

Because the method relies only on the file's binary makeup, it can extend to spreadsheets, models, AR/VR environments, CNC machine code — or file types not yet imagined.

With this depth, files are not just intact — they are tied to the people and authority behind them, and remain verifiable years later.

The contrast is simple:

- DSS protects the file integrity.
- CONCERT protects the file, the signer, and the authority behind it.

Span of the Project Lifecycle

This section completes the triad alongside depth and breadth. Just as depth secures the author and breadth secures every format, span ensures that protection extends across the entire project lifecycle.

Today's system stops at construction documents. A digital signature may be applied to a stamped plan set for permitting, and that becomes the official record. But projects are built on much more than stamped drawings.

Critical decisions flow every day in RFIs, field directives, change orders, schedules, emails and owner communications. These exchanges often drive scope, cost, and liability even more than the stamped drawings themselves. Yet none of them are secured by the current trust model.

They are scattered across in-boxes, file shares and portals — important enough to change the course of a project, but unverifiable if challenged.

CONCERT closes that gap. The same trust backbone that secures final drawings also secures everyday exchanges. RFIs, memos, schedules, and directives can all be authorized and recorded in the same way as plan sets. This creates a continuous chain of accountability that stretches across the entire project lifecycle.

For firms, the benefit is clear:

- ☒ **Less risk.** When disputes arise, every important exchange has an auditable record.
- ☒ **More efficiency.** Project teams spend less time hunting for "the official version."
- ☒ **Greater trust.** Owners and contractors see that commitments are real, not just words in an email.

Instead of covering only a sliver of the project, the **whole project lifecycle is protected.**

The contrast is simple:

- DSS protects construction documents.
- CONCERT protects the entire project.

Digital Authorization vs. Digital Notarization

It is essential to distinguish between digital authorization and digital notarization in CONCERT. These fit naturally alongside depth, breadth, and span by clarifying the context in which each form of trust applies.

Digital Authorization (DA). Applies to any file type in CONCERT that is recorded into a blockchain record. This could be:

- ☒ A file shared without needing review
- ☒ A file shared with acknowledgment of receipt
- ☒ A file that moves through collaboration and results in a definitive authorized version

  DA does not require a sign & seal, does not include MFA protections, and is not necessarily tied to licensure. It is a flexible mechanism for everyday project data

Digital Notarization (DN). Reserved for items typically reviewed by external authorities such as permitting or planning departments. These files require the higher bar of sign & seal, MFA protection, and validation of licensure. They form the authoritative record for regulatory and legal purposes.

Best Practices Using DA & DN

Use DN for documents that carry the full weight of a licensed professional's responsibility. These typically include construction documents submitted to permitting authorities, as well as major submittals that serve as replacements for sealed drawings.

Use DA for files that must be recorded, shared, or acknowledged but do not need the formal protection of notarization. Examples include collaborative exchanges, shared references, or deliverables acknowledged between project partners.

No DA or DN needed for works-in-progress. Drafts passed back and forth between authors and editors generally fall outside the scope of CONCERT's protections until they reach a stage where authenticity, authorship, or authority needs to be verified.

A NOTE OF CLARIFICATION

CONCERT is not a Notary Public. Official notarial acts generally involve specific statutory requirements that vary by state but often include four common elements:

1. Verifying the identity of the signer, typically through government-issued identification.
2. Ensuring the signer appears in person before the notary (personal presence).
3. Confirming the signer's willingness and awareness (no coercion or incapacity).
4. Maintaining a record of the act, usually in a notarial journal, and affixing an official seal.

These requirements are set out in state statutes and coordinated nationally through the National Notary Association (NNA), which provides guidance and model standards. While CONCERT provides online processes that mirror some notarial functions, it does not act as a notary public in person or online.

Conclusion

Taken together, depth, breadth, and span transform a limited, document-only model into a comprehensive system of trust. Files are still sealed the way regulators expect, but the protection now runs deeper — linking every authorization to the person, their license, and an immutable record. It runs broader — covering all file format, not just PDFs. And it runs farther — extending across the whole span of the project lifecycle, from plan sets to everyday exchanges.

Alongside this three-dimensional trust, CONCERT distinguishes between digital authorization for everyday files and digital notarization for those carrying the full weight of professional responsibility. This dual approach ensures that trust is applied in ways that fit the context: flexible when collaboration demands speed, and rigorous when regulators demand certainty.

The outcome is a coherent framework that builds upon legal and technical foundations, adapting them to the modern method of design and construction. Trust extends beyond the narrow lane of PDFs to encompass the full diversity of project deliverables, preparing firms for future formats — including robotic instructions and other machine-readable assets.

The result is simple but profound:

CONCERT protects projects, not just documents.