

PRONETWORK NEWS

Risk Management Tools for the Design Professional

COMPANY NAME HERE

September 2026 | Vol. XXIX No. 1159



Nada Belhadfa

Ms. Nada Belhadfa is Vice President, Professional Ecosystems at Portage CyberTech, where she leads strategic partnerships, go-to-market (GTM) strategy, market expansion, and key account management across Canada and the United States.

With more than a decade of experience in business development, strategic alliances, and regulated professional ecosystems, she works closely with regulators, professional associations, governments, and industry leaders to advance trusted digital transformation initiatives.

Her expertise spans digital identity, electronic signatures, verifiable credentials, and policy development, helping organizations navigate regulatory frameworks while accelerating the adoption of secure digital trust solutions.



a/e ProNet
Lynda Colucci, Executive Director
info@aepronet.org

Signed, Sealed and Unverified

The Identity Risk Behind Electronic Signatures and Why It Matters to a/e ProNet Members

By Nada Belhadfa, VP Professional Ecosystems

A professional seal has always meant something. It tells a client, regulator, lender, or member of the public that a licensed professional stands behind the work and can be held accountable. But in a digital workflow, what looks like a seal may be nothing more than an image on a PDF. If that image can be copied or separated from the signing process, it may no longer prove who approved the document, whether that person was authorized to sign it, or whether the document changed afterward.

That disconnect is where risk begins. For a/e ProNet members and their architecture and engineering firms, that gap creates a practical risk: when identity, authority, and document integrity cannot be verified, claims become harder to investigate, and disputes can begin before the quality of the work is even considered.

AI Has Industrialized Document Fraud

AI has made it easier to create convincing documents, identities, and credentials. Professional seals and signatures are no exception. The real question is not whether a document looks authentic, but whether the identity, authority, and integrity behind it can be verified.

When Seal Misuse Becomes a Professional Liability Risk

Recent cases show the risk is real. The Florida Board of Professional Engineers reported allegations involving another engineer's PE number, a deceased parent's seal, and fabricated digital seals. In California, employees were convicted for using an employer's seal and signature without permission. Another federal case involved the alleged use of licensed engineers' names and stamps on fraudulent inspection reports.

Once a seal is challenged, the issue is no longer only professional judgment. It becomes an evidence question: Who signed? Under what authority? Can the document's integrity be demonstrated?

PRONETWORK NEWS

Risk Management Tools for the Design Professional

RECENT BLOG POSTS

Congratulate the 2026–2027 ACEC
a/e ProNet Engineering Scholarship
Recipient: Sabah Naji [Read More](#)

Congratulate the 2026–2027 David W.
Lakamp Architect Scholarship
Recipients: Ingram Lucier and Lily
Wang [Read More](#)

Finding Community and Confidence
Through Conferences [Read More](#)

Celebrating the 2025–2026 David W.
Lakamp Architect Scholarship
Recipients: Anna Turco and Rosalyn
Becicka [Read More](#)

Celebrating the 2025–2026 a/e ProNet
ACEC Engineering Scholarship Recipient:
Avery Michaels [Read More](#)

A Conversation with Alexandra Gottlin
2021–2022 David W. Lakamp AIA
Scholarship Recipient [Read More](#)

Project Update From Kaitlin Pickart a/e
ProNet David Lakamp Architect
Scholarship Recipient [Read More](#)

PRONETWORK NEWS

May 2026 - New Claims Benchmark
Report: Insights to Help Design
Professionals Manage Risk [Read More](#)



a/e ProNet
Lynda Colucci, Executive Director

info@aepronet.org
aepronet.org

Not All Electronic Signatures Are Equal

A scanned signature, a pasted seal image, and a certificate-based digital signature may look equally official, but they do not carry the same legal weight from a burden of proof perspective despite being all valid ways to sign. Many electronic signature tools capture intent to sign without independently confirming an active license, professional standing, or signing authority. A signature may be legally valid and still leave critical questions unanswered when a claim arises.

A professional digital signature adds independent verification. A Certificate Authority verifies identity, while a Registration Authority, such as a professional licensing body, validates professional status. The resulting credential links the signer to the document and makes post-signing changes detectable.

Four Questions That Make Document Risk Easier to Assess

Four simple questions can be used to assess whether a signed document will withstand scrutiny. They are not technical questions. They are governance and risk questions:

Identity and authority: Who signed, and in what professional capacity?

Integrity: Can changes made after signing be detected?

Authenticity: Is the proof of signing bound to the document itself?

Longevity: Can the signature and credential still be verified years later?

In underwriting and claims terms, these questions address attribution, change control, evidence quality, and long-term reliability. If any one of them cannot be demonstrated, confidence in the document begins to erode.

What This Means in Practice

For brokers and insurers

- At renewal, ask how professional signing credentials are issued, protected, controlled, and revoked. Asking whether the firm uses electronic signatures is not enough.
- At underwriting: treat document authorization and integrity as genuine risk controls, alongside established quality-assurance and quality-control procedures.
- At claims intake: identify what evidence is available to verify the signer's identity and authority and to detect any changes made after signing.

PRONETWORK NEWS

Risk Management Tools for the Design Professional

For architecture and engineering firms

- Confirm that your signing process produces independent, verifiable proof of who signed, not simply an image of a seal.
- Protect digital signing credentials as you would protect a physical stamp or license number.

Put simply, if trust cannot be proven, it becomes a liability.

Three Questions Worth Asking Before Insuring the Work

At renewal or during a risk review, three questions can quickly reveal how much a firm really knows about its signing process:

- How do you prevent unauthorized reuse of seals and signatures?
- Can you prove a signed document has not been altered, even years later?
- Are signing credentials issued and independently verifiable through a trusted professional framework?

Trust should not be assumed. It should be verifiable.

To learn more about professional digital signatures and our free signature-validation tools, scan the code below or visit portagecybertech.com.



PORTAGE CYBERTECH | DOCUMENT TRUST

Sources

Florida Board of Professional Engineers, Look Out for Engineering-Related Forgeries (2024),
<https://fbpe.org/look-out-for-engineering-related-forgeries/>.

People v. Rodriguez, 71 Cal. App. 5th 921 (2021),
<https://law.justia.com/cases/california/court-of-appeal/2021/b305512.html>.

Press Release, U.S. Attorney's Office, N.D. Cal., Former Bay Area Engineer Charged With Mail Fraud and Aggravated Identity Theft in Connection With Fraudulent Building Inspection Reports (July 22, 2020)
<https://www.justice.gov/usao-ndca/pr/former-bay-area-engineer-charged-mail-fraud-and-aggravated-identity-theft-connection>.



a/e ProNet

Lynda Colucci, Executive Director

info@aepronet.org
aepronet.org