White Paper

# The AI Amplification of the Digital Trust Problem

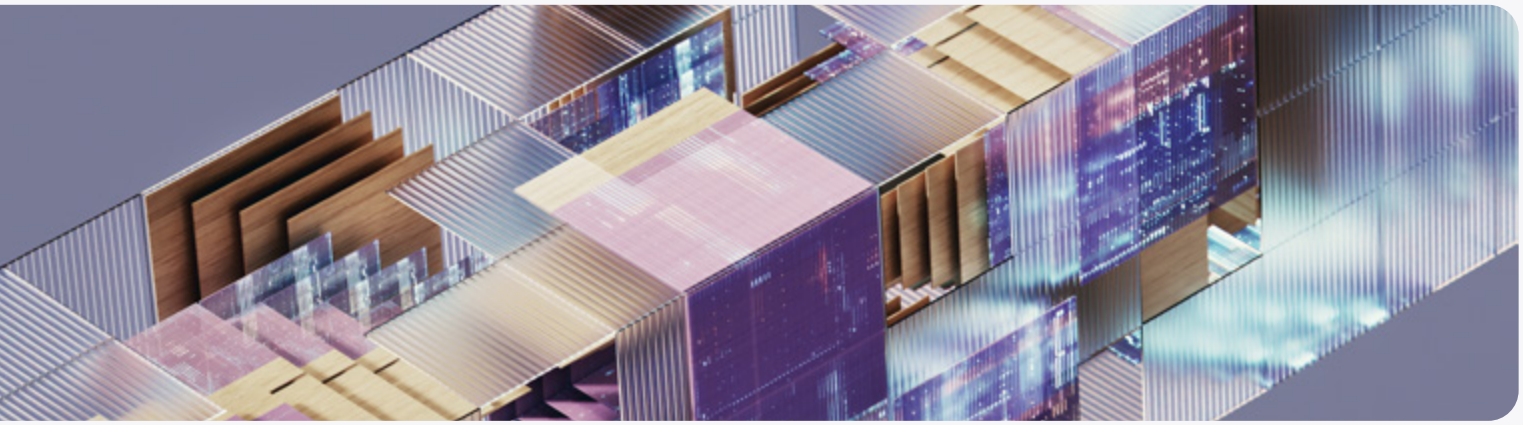
**Why connected identity, trusted transactions, and verifiable data must come before responsible AI**

PORTAGE cybertech

portagecybertech.com
info@portagecybertech.com

Executive Summary

# AI will not fix fragmented trust. It may scale it.



From drafting a quick email to choosing a new restaurant or planning a multi-country trip, many of us now turn to an AI assistant before turning to another person. Whether through ChatGPT, Claude, Gemini, or Copilot, AI has moved from novelty to necessity in a remarkably short time.

Governments and regulated organizations feel the same pull. Citizens, customers, and employees expect faster, more personalized digital services, while leaders are asked to improve efficiency, control risk, and do more with limited resources. AI can help route cases, summarize evidence, detect patterns, accelerate transactions, and support decisions in ways no human team could match. That potential is real. So is the pressure to move quickly. The danger lies in confusing speed with readiness.

AI is a force multiplier, not a repair crew. It cannot fix fragmented identity, disconnected workflows, weak evidence, or unverified data simply by sitting on top of them. In fact, it may make those cracks harder to see while compounding their effects even further.

Successful AI integration depends on connected context. Yet many organizations lack that context. Users must prove who they are again and again. Critical transactions remain manual, paper-heavy, or legally unreliable. Data is siloed across systems, programs, and jurisdictions. These are the experience, process, and infrastructure failures that erode digital trust and sharply increase the risks of deploying AI at scale.

Responsible AI therefore has to begin before the model. It begins with digital trust: the ability to establish who or what is acting, apply the right level of assurance, authorize the action, protect the transaction, verify the document or output, preserve the evidence, and support sound decision-making.

The goal is a continuous chain from identity proofing to action to outcome. With that chain in place, AI can improve service delivery while accountability, legal reliability, and public confidence remain intact. Without it, AI will only automate uncertainty.

# #1 The Digital Trust Problem Was Already Here

## Fragmented systems create fragmented trust.

Digital transformation has delivered some impressive tools, but not always a coherent experience. A polished web form on the front end may still involve several accounts, manual re-entry, emailed attachments, and a heroic amount of institutional memory to complete a single transaction.

Citizens, customers, businesses, and professionals do not experience those back-end systems. They experience one journey. When they must re-prove identity, submit the same information twice, jump between services, or lose track of what happened to a signed document, internal silos become visible as friction. Repeated often enough, users begin to wonder whether anyone is in charge.

This is why digital trust is broader than technology alone. It is the expectation that people, processes, systems, and evidence will work together as intended. Leading trust frameworks treat digital trust as an ecosystem capability built on interoperability, privacy, security, governance, and reliable evidence.

**Three failures reinforce one another:**

- **Experience failure:** users lose confidence when services are inconsistent and difficult to navigate.
- **Process failure:** paper-heavy, inefficient, or opaque workflows weaken accountability.
- **Infrastructure failure:** disconnected systems and siloed data prevent trusted outcomes across organizations and jurisdictions.

**As trust breaks down, friction increases and confidence erodes.**

# #2 AI Changes the Scale of the Problem

## AI makes fragmented trust move faster, but not better.

AI can improve an isolated service experience, but it cannot automatically connect identity across fragmented services. A chatbot may answer a question beautifully while the user still needs three accounts to finish the task.

AI can also speed up a transaction, but speed does not tell the system whether the right person is acting, whether they have authority, or whether the action requires stronger assurance. Those questions must be designed into the workflow.

AI can generate recommendations, route cases, and flag risk. But when the underlying data is incomplete, unverified, or disconnected, the resulting output may be difficult to explain, challenge or audit.

The biggest risk is not simply that AI makes a mistake. It is that existing fragmentation becomes automated, less connected, and harder to unwind. A bad decision made once is a problem. The same decision, applied across thousands of cases without the proper level of assurance and trust—and before anyone can reconstruct why it happened—is a much bigger one. That is how weak foundations create worse outcomes, faster.

**Automation is wonderfully impartial. It will repeat a bad process with exactly the same enthusiasm as a good one.**

# 3 AI Raises the Evidence Standard

**Trust can no longer depend on appearance, convenience, or isolated audit trails.**

AI has lowered the cost of producing convincing documents, reports, contracts, drawings, seals, and even digital impersonations. A clean layout, familiar logo, or realistic signature image may look reassuring. Unfortunately, appearance is now one of the easiest things to manufacture.

**In the AI era, visual credibility is no longer proof of authenticity. High-risk signing workflows need to establish three things:**

1. **Verified identity:** Who signed, approved, submitted, or produced the record?
2. **Document integrity:** Has the content changed since the trusted action occurred?
3. **Durable evidence:** Can the proof still be validated years later?

**Public guidance on generative AI and synthetic media reinforces the importance of stronger controls around identity, provenance, and evidence.**

Content provenance standards, such as C2PA, can help show where digital material came from and how it changed. Digital signature trust programs and long-term validation standards, such as the Adobe Approved Trust List and ETSI PAdES, can help protect integrity, connect a signing action to the signer, and preserve verifiable evidence over time. Each addresses one part of the problem, but the full trust chain still depends on identity, authorization, the transaction record, and durable proof working as one.

The signing workflow matters just as much as the finished file. A basic electronic signature may be perfectly suitable for low-risk consent. A regulated approval, professional drawing, public record, or high-value transaction may require verified identity, stronger authentication, certificate-backed signing, tamper evidence, and long-term validation. The level of assurance should be commensurate with the consequence.

**The question has changed from "Can we do this online?" to "Can we prove who did it, what happened, and whether the evidence still holds up?"**

# 4 Identity Must Become the Foundation

**Before AI can act responsibly, organizations must know who or what is involved.**

Identity is the starting point of trusted context. It should determine access decisions, transaction authority, signing rights, data use, and the assurance attached to the resulting outcome.

That does not mean applying maximum friction everywhere. NIST's Digital Identity Guidelines distinguish identity proofing, authentication, and federation, and support assurance choices that reflect risk. Low-risk interactions should stay simple. Higher-risk actions should trigger stronger verification, authentication, authorization, or signing controls. Not every door needs a bank vault. The important part is knowing which doors lead to one.

The W3C Verifiable Credentials Data Model provides a standards-based way for issuers, holders, and verifiers to exchange tamper-evident claims. Reusable credentials can carry verified information across services without forcing people to start from zero each time. This enables a more seamless journey while keeping assurance tied to policy and risk.

**A practical identity-first progression is:**

1. Vet and establish identity
2. Issue and bind credentials
3. Establish, federate and exchange trust
4. Apply the appropriate assurance level
5. Assess risk and trustworthiness
6. Orchestrate trust interactions
7. Enable the evidence base for trusted decisions

Identity is not the whole digital trust model, but it anchors everything that follows. Once identity and assurance are established, that context can carry into access, transactions, documents, evidence, and decisions.

## When AI is an Actor in the Workflow

As AI moves from generating content to taking action, some agents may need their own governed, non-human identity (NHI). Unlike human users, whose access is typically tied to a known person and role, AI agents may interact with multiple systems, APIs, and data stores while acting under delegated authority. This creates a larger, more complex identity footprint that requires carefully scoped access and a clear delegation path.

This does not make AI a person or transfer accountability away from humans. It ensures the organization can identify the agent, define its permissions, limit its reach, record who granted its authority, audit what it did, and revoke access when necessary.

In high-risk workflows, an AI agent should not be invisible or indistinguishable from the person or organization it supports. The agent may have an identity and permissions, but accountability must remain with the responsible human and organization.

# #5 The Connected Digital Trust Model

**Identity, transactions, and trusted data must mature together.**

Connected digital trust brings these elements into a single operating model rather than treating them as separate tools. Continuous identity, reliable transactions, and trusted data exchange are three mutually reinforcing capabilities that enable responsible AI and more confident decision-making.

**Continuous identity**

Users move across services with trusted, reusable identity and credentials.

**Reliable transactions**

Workflows become risk-aware, authorized, auditable, and legally reliable where required.

**Trusted data exchange**

Verified information moves across systems, organizations, and jurisdictions with provenance, consent, and policy intact.

**Responsible AI and better decisions**

Trusted context supports safer automation, verifiable outputs, and accountable decision-making.

**As these capabilities become more integrated, AI can improve experiences, assess risk, automate services, generate trusted outputs, and support more informed decisions. It acts on reliable context, with human oversight, auditability, and stronger evidence available for review.**

## A Converging Digital Trust Landscape

**Different sectors are arriving at the same digital trust crossroads.**

Identity providers are extending into AI-agent authorization. Digital signing platforms are adding identity verification and workflow intelligence. Enterprise platforms are embedding AI agents into business processes and data environments. Trust-service, provenance, and governance providers are strengthening proof of the integrity and authenticity of systems, content, and data.

This convergence shows that trust is becoming an essential control layer around AI-enabled workflows. It also exposes a gap: many approaches still begin and end with the part of the technology stack they already own.

Governments and regulated organizations rarely operate within a single platform. Their services cross departments, vendors, professions, organizations, and jurisdictions. Trust therefore needs to travel with the person or agent, the transaction, the document, the data, and the evidence.

Model governance and workflow automation are important, but neither can create evidence that the underlying process never captured. Identity, transactions, documents, and trusted data must operate as one coherent trust model.

# 6 Responsible AI Requires Human Accountability

**AI recommends or acts. Humans remain accountable. Evidence stays connected.**

Responsible AI is often discussed in terms of the model: fairness, safety, explainability, and robustness. Those qualities matter, but they do not govern the full workflow. They do not show who authorized and/or committed an action, what data shaped it, what transaction followed, or whether the resulting document remained intact.

Canada's Directive on Automated Decision-Making applies not only to fully automated decisions, but also to recommendations, scores, summaries, and other outputs that contribute to administrative decisions. The OECD AI Principles likewise emphasize transparency, traceability, robustness, and accountability. For agentic systems, the World Economic Forum describes governance in terms of delegated decision rights and enforceable boundaries. Accountability must extend beyond the model to the workflow around it.

A "human in the loop" is not a governance strategy. If the human receives an opaque recommendation, has no meaningful ability to challenge it, and leaves no connected record of the decision, the loop may be little more than a formality.

**Responsible workflows should preserve a traceable chain:**

- who or what acted;
- who authorized the action;
- what data and policy were used;
- what transaction, recommendation, or document resulted;
- what human review occurred;
- what evidence remains.

Within clear, governed limits, AI may recommend or act. People and institutions remain accountable for the service, the policy, and consequences. The evidence should make that accountability visible.

**Responsible AI is only as trustworthy as the identity, transaction, data, and evidence it relies on.**

# #7 From Fragmented Services to Verifiable Outcomes and Better Decisions

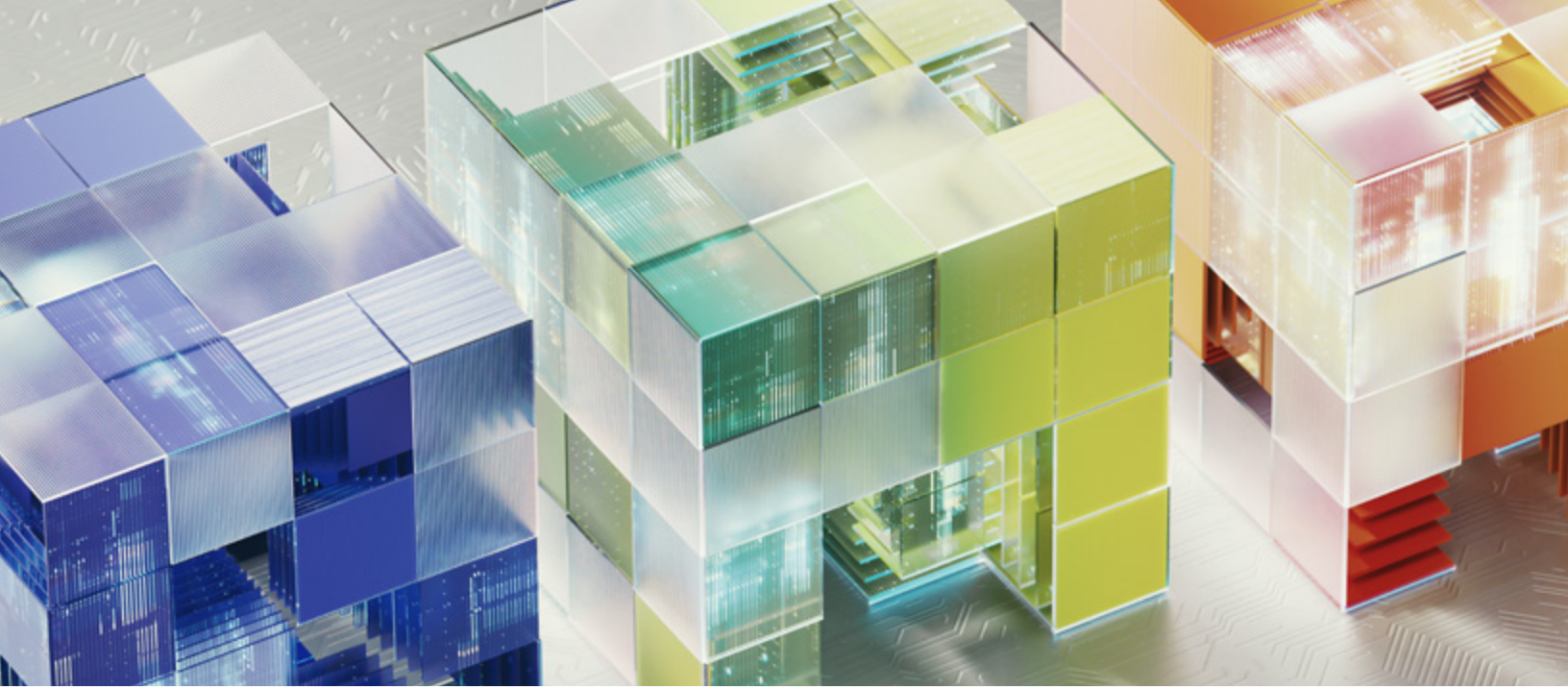
## A maturity path for trusted digital transformation and decision-making.

Connected trust develops in stages. Organizations do not need to rebuild everything at once, but each step should make the next one safer, more efficient, more useful, and easier to govern.

| Stage | Trust capability | AI value unlocked |
|---|---|---|
| **Consolidate access** | One identity across services | AI can support a more seamless user journey. |
| **Digitize transactions** | Reliable, auditable workflows | AI can assist without losing accountability. |
| **Enable trusted credentials** | Reusable identity evidence and credentials | AI can personalize or route services using stronger context. |
| **Personalize services** | Consent, preferences, eligibility, and identity context | AI can support relevant recommendations without relying only on fragmented assumptions. |
| **Apply risk-based assurance** | Assurance matched to risk | AI can help assess context and trigger appropriate controls. |
| **Automate eServices** | Clear rules, authorization, and auditability | AI can reduce friction while preserving accountability. |
| **Enable trusted data exchange** | Verified data between systems | AI can act on better information. |
| **Enable better decisions** | **Trusted identity, verified data, auditable transactions, and durable evidence connected across the service journey** | **AI can support recommendations and decisions based on stronger context, while humans retain accountability.** |

**Verifiable outcomes are not the finish line. They provide the evidence base for stronger decisions. When an organization can trust who is involved, what they are authorized to do, what data was used, what was signed or approved, and what proof remains, both humans and AI-enabled systems can act with greater clarity and context.**

**Decision quality does not come from a clever model alone. It depends on trustworthy inputs, clear rules, reliable transactions, and evidence that can stand up to review.**



# 8 The Portage CyberTech Perspective

## A connected trust foundation for governments and regulated organizations.

**Portage CyberTech helps governments and regulated organizations connect digital trust across the full service journey.**

That foundation can begin with CitizenOne, a government-grade CIAM platform that supports trusted identity and secure access across services and channels. CertifiO ID adds high-assurance identity verification matched to transaction risk. CertifiO ties a verified individual and, where applicable, professional affiliation to a highly assured digital signature. ConsignO Cloud supports secure signing workflows, configurable assurance, document integrity, and audit evidence.

**The value is not the product sequence. It is the continuity of trust:**

**Verified identity** → **Appropriate assurance** → **Authorized action** →
**Trusted document** → **Durable evidence** → **Defensible decision**

Portage brings these trust requirements into one operating model: vetting identity and associating it with a person or agent; linking that identity to what they may access, sign, approve, or initiate; defining the evidence a regulated workflow must preserve; and enabling trust to carry across organizations and jurisdictions.

For public-sector and regulated services, that connective tissue turns automation into accountable service delivery and trusted outputs into defensible action.

# #9 What Leaders Should Do Next

## Assess where AI could amplify existing trust gaps.

**Before scaling AI, map the trust chain around the workflows it will touch. Ask:**

1. Can you confidently verify that each user is tied to a proven individual?
2. Where do users still need separate accounts, repeated identity checks, or disconnected credentials?
3. Which transactions require stronger assurance because of risk, value, sensitivity, or legal consequence?
4. Which document workflows rely on appearance, PDFs, or thin audit trails instead of cryptographic proof?
5. Where is data fragmented between systems, organizations, or jurisdictions?
6. Where could AI automate a broken process instead of improving the outcome?
7. Which decisions, recommendations, signatures, or approvals need durable evidence?
8. What level of assurance should apply to each major service or workflow?
9. Where might AI agents require their own governed identity, scope, delegation, auditability, or revocation path?
10. Which decisions would improve if identity, transactions, data, documents, and evidence were linked across the workflow?

Then prioritize the services where identity, transactions, documents, data, and AI intersect. Strengthen the trust chain before increasing the speed.

AI will transform digital service delivery. The organizations that benefit most will be those that can verify who or what acted, confirm the authority behind the action, trace the data and transaction, preserve the document and evidence, and use that context to act with greater confidence.

## Appendix: References and Source Notes


1. National Institute of Standards and Technology (NIST). AI Risk Management Framework (AI RMF 1.0). Primary risk-management framework.
2. World Economic Forum. Measuring Digital Trust: Supporting Decision-Making for Trustworthy Technologies. Executive digital trust framework.
3. Digital ID & Authentication Council of Canada (DIACC). Pan-Canadian Trust Framework.
4. National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). Generative AI risk guidance.
5. NSA, FBI, and CISA. Contextualizing Deepfake Threats to Organizations. Synthetic media threat guidance.
6. Coalition for Content Provenance and Authenticity (C2PA). C2PA Technical Specification. Content provenance standard.
7. Adobe Approved Trust List. Certificate trust infrastructure for digital signatures.
8. European Telecommunications Standards Institute (ETSI). PAdES Long-Term Validation Profile (ETSI TS 102 778-4). Digital signature validation standard.
9. National Institute of Standards and Technology (NIST). Digital Identity Guidelines, SP 800-63-4. Identity proofing, authentication, and federation guidance.
10. World Wide Web Consortium (W3C). Verifiable Credentials Data Model v2.0. Technical standard for verifiable claims.
11. Government of Canada. Guide on the Scope of the Directive on Automated Decision-Making. Public-sector decision and accountability guidance.
12. Organisation for Economic Co-operation and Development (OECD). OECD AI Principles. International principles for trustworthy AI.
13. World Economic Forum. From Systems of Record to Systems of Trust: A Board-Level Playbook for Governing Agentic AI. Executive guidance on delegated decision rights and governance boundaries.

# Connect Digital Trust Across Your Organization

**Portage CyberTech can assess where AI could amplify gaps across identity, transactions, documents, data, and evidence.**

As a provider of connected digital trust solutions for governments and regulated organizations, we help strengthen the foundation for responsible automation, verifiable outcomes, and accountable decision-making.

**Contact Portage CyberTech for an AI-era digital trust assessment.**
https://www.portagecybertech.com/en/contact

# Next Steps?
# Questions?

**Learn more about**
**Portage CyberTech's solutions.**

**Or book a consultation with one of our experts if you're ready to explore how our solutions can benefit your municipality.**