

RKVST

MAKE DATA TRUSTWORTHY

**DIGITAL CONTENT
INTEGRITY, AUTHENTICITY
& TRANSPARENCY**

INTRODUCING RKVST



JULY 2023

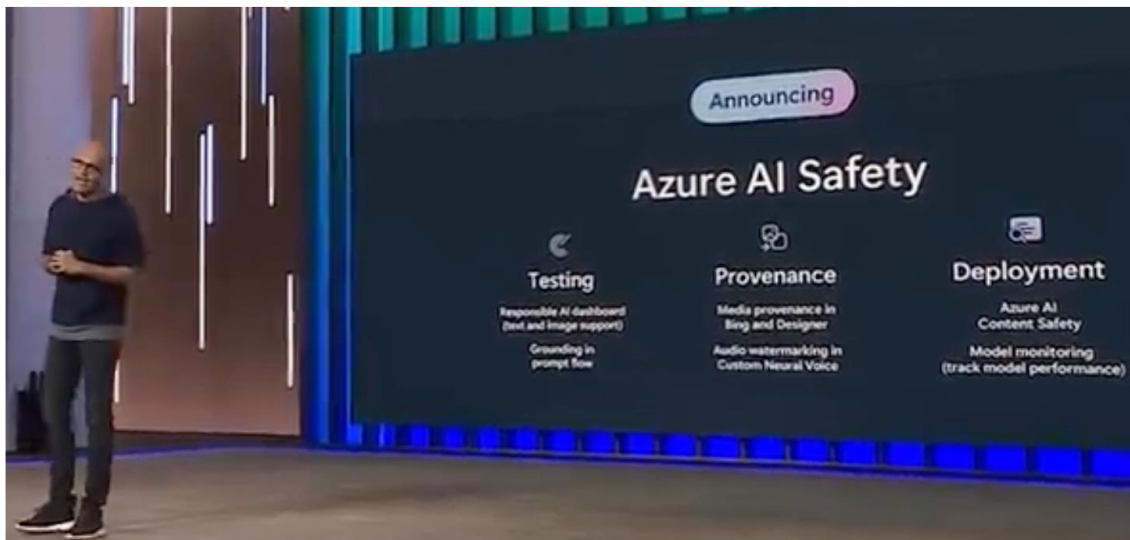
DIGITAL CONTENT INTEGRITY, AUTHENTICITY AND TRANSPARENCY

As supply chains continue to evolve and new AI technology becomes part of every business, traditional trust systems that rely on human interactions to verify and validate data will struggle to keep pace. Digital supply chain practices from media through software to physical goods must adapt to this changing global technology landscape.

Recently, the BBC introduced its new BBC Verify service to validate digital content. That service includes a team of 60 people, which unfortunately is not the type of adaptation every business can afford.

The innovations unleashed in GenAI have made it apparent that we can no longer trust what we see and read; we must verify data before we use it. In other words: if data is the fuel of your business and your new AI systems, then you need to make sure you are running on clean fuel from verified sources.

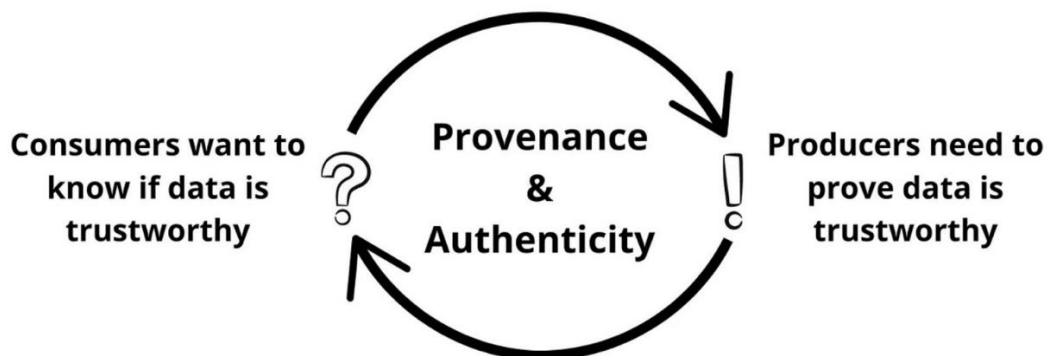
Satya Nadella, CEO Microsoft, identified AI safety as the most urgent problem that needs to be addressed today and highlighted data provenance as the essential component.



LET THE DATA FLOW...SAFELY

Typical approaches to IT security have focused on silos, perimeters and encryption: keeping secrets in and other people out. But AI and data-driven businesses *require* the flow of data between partners. We need to switch the security focus to integrity and authenticity: letting data flow, and always ensuring you know exactly where it came from. Knowing the data

you receive is truly the data that was sent, and that the sender can be held accountable for their actions will make lasting improvements and changes in the way we decide what data to trust. However, for this to work there needs to be a base layer of agreement; we need standards that enable businesses to instantly prove and verify digital content.



In this era of generative AI the fakers have the upper hand: while defense relies on scaling up teams, attacks scale at the press of a button. To safely continue the rapid digitization of the world we need a common provenance format that captures origin, authenticity and lineage information, and exposes digital fakes or tampering. We *also* need a better trust model that adds integrity, transparency, and trust to all data.

Fortunately, communities at the Internet Engineering Task Force (IETF) and Linux Foundation have come together to create those standards. The IETF is working on data integrity, transparency and trust standards for all supply chains (SCITT) and the Linux Foundation is working on digital content provenance and authenticity standards under the Coalition for Content Provenance and Authenticity (C2PA) specifically for media content.

A BETTER MODEL FOR DIGITAL TRUST

At RKVST, we started several years ago on a better model for digital trust and we now have a leadership role in defining the SCITT architecture and the standards for data integrity and transparency for the modern world.

We're also working with Microsoft, ARM and many other companies to build a SCITT community with open source tools supporting the standard for anyone to use. RKVST is also a member of the Content Authenticity Initiative (CAI) alongside over 500 other companies, including Adobe and Reuters, working on open source provenance metadata creation tools.

For each of us to make a decision about what data to trust, we need cryptographically signed, verifiable proof *plus* a distributed ledger with an append only model that can be instantly verified. Transparency ensures the mutual accountability, non-repudiation, and non-equivocality necessary to make AI safer and digital supply chains more efficient and worthy of our trust.



<https://www.youtube.com/shorts/SPnWeOHvRMo>

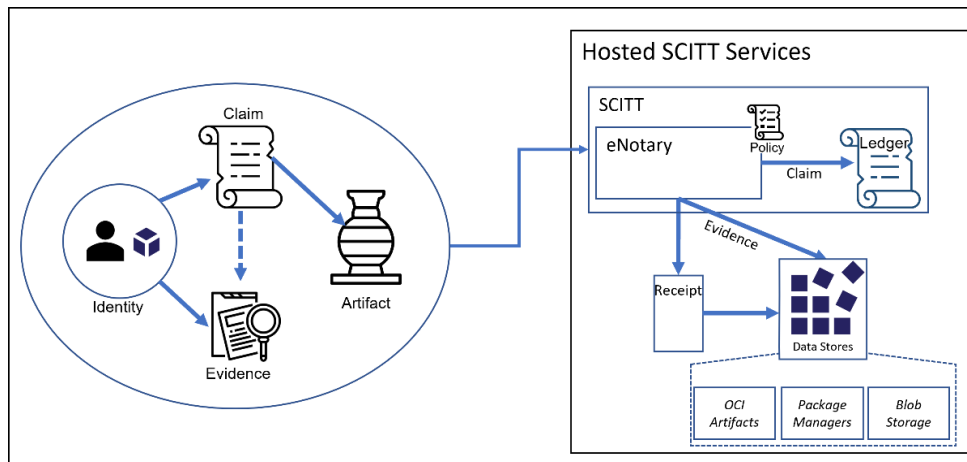
THE SCITT ARCHITECTURE AND ENHANCED TRUST MODEL

With cracks in the current digital trust system only growing deeper, the IETF chartered the Supply Chain Integrity Transparency and Trust (SCITT) working group to create a new and enhanced digital trust model that everyone can rely on.

SCITT is an industry-standard approach to attest and validate supply chain data, focused on defining the essential building blocks that make up a trustworthy open architecture for the

exchange and verification of any supply chain artifact. The standard provides a consistent interoperable framework where the legitimacy of entities, evidence, claims, and artifacts can be firmly established.

SCITT ensures that the actions of these entities are authorized, non-repudiable, immutable, and auditable, setting the foundation for a trustworthy digital ecosystem both for real-time decision-making and long-term auditability.



SCITT will significantly improve the transparency and integrity of digital operations. It works similarly to a digital notary service, by storing verifiable claims on a distributed ledger, recording information about the artifact and its supporting

evidence. As supply chains continue to evolve and become increasingly complex, applications built on the SCITT building blocks will lay the foundations for a more secure and trustworthy digital world.

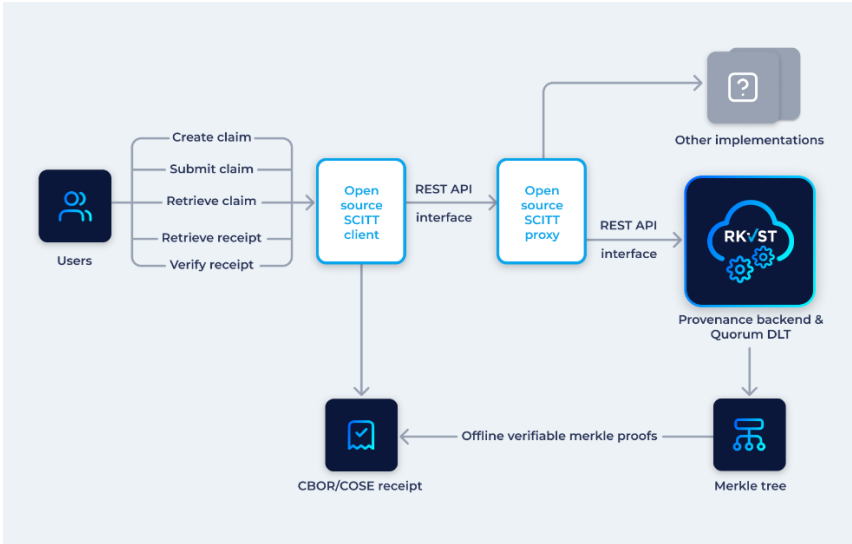
RETHINKING TRUST: INTRODUCING THE RKVST PLATFORM

RKVST is an API-first platform that offers a robust solution to enhance and protect trust in digital content and evolving supply chains. By separating data from provenance metadata, enforcing rules through cryptography, and leveraging distributed ledger technology, RKVST empowers all supply chain partners to collaborate

effectively, ensure transparency, and establish a single source of truth. RKVST enables instant data authentication by capturing and maintaining provenance metadata while enforcing sharing and visibility rules through cryptography and intuitive attribute-based access controls.

Data sources in RKVST include:

- **Entities:** These are parties involved in the supply chain that generate information about the goods and services being processed
- **Artifacts:** physical or digital items produced as part of supply chain processes that describe or contain the results of supply chain processes. Artifacts comes in different forms, such as documents, receipts, logs, bills of materials, certificates, images, or plain JSON data.
- **Evidence:** Strongly protected and verifiable data that builds reputation and trust in artifacts by notarizing claims made by Entities about Artifacts.



MAKE DATA TRUSTWORTHY

To ensure trust in these data sources, RKVST includes several elements of verifiable provenance:



First, identity verification is a critical step that requires entities to be identifiable and verifiable, substantiating the claims or evidence they provide. This level of transparency strengthens the trust in the entity and its data.



Data authenticity is confirmed by enabling auditable trails of data origin and evolution, ensuring that the data genuinely comes from the declared source and is the correct and latest version published by the source.



To further fortify this trust, RKVST ensures data integrity by guaranteeing that the data from these sources remains non-repudiable and immutable, preventing equivocation of statements and protecting evidence against unauthorized alterations or tampering during transmission or storage.




To maintain a consistent and reliable data environment, RKVST employs a transparent and auditable ledger. This ledger can be cross-checked by anyone with standard OSS tooling, making the RKVST system tamper-evident even against RKVST itself.

Extensive data governance features are included in the platform that provide fine-grained access controls for sharing provenance both privately and publicly. Original data never needs to enter the RKVST system so sensitive business secrets can remain in your existing archives on-prem and in the cloud whilst still benefiting from globally verifiable provenance and integrity. By combining confidentiality, integrity and availability, RKVST creates a robust basis for enhancing and maintaining trust in the data content and sources that underpin all digital operations .

MAKE DATA TRUSTWORTHY

RKVST BENEFITS

As AI technology and digital supply chains continue to evolve, the adoption of RKVST will contribute to improved efficiency, resiliency, and transparency between businesses, partners, and customers and safety in AI.



- Retain and gain trust online**
- Eliminate manual 3rd party data validation**
- Save time and money on R&D and DevOps**



AVIATION CARBON TRACKING

**18+ MONTHS
R&D SAVINGS**

-  Instant value
-  No expert DLT skills required
-  Efficient scalability



NUCLEAR SUPPLY CHAIN

**25 YEARS
OPEX SAVINGS**

-  90% Greater data accuracy
-  55% Process improvement
-  25% Processes automated

LEDGER FOR ESG ACCOUNTING

BUY BEATS BUILD

Build themselves: spend time and money outside of core business activities.

- Build vs buy R&D decision.
- High risk and no expert staff
- Ongoing maintenance burden

Buy RKVST: add provenance in a single API call.

- Onboarded in minutes.
- Expert integration support
- Automatically keeps up with tech.

TRACK & TRACE NUCLEAR WASTE

UNLEASH THE POWER OF DIGITAL OPERATIONS

BEFORE: Trust **but** verify legacy processes

- Multiple supply chain data steps
- Multiple data replications
- Multiple audits and cross-checking

AFTER: Verify **then** trust using RKVST

- Real-time traceability and auditability
- Single source of truth for multi-party operations
- Fast remediation and issue prevention

REFERENCES

Internet Engineering Task Force Supply Chain Integrity, Transparency and Trust: <https://scitt.io/>

Coalition for Content Provenance and Authenticity: <https://c2pa.org/>

Content Authenticity Initiative: <https://contentauthenticity.org/>

Digital Catapult Sellafield DLT Field Lab:

<https://www.digicatapult.org.uk/expertise/publications/post/harnessing-the-power-of-distributed-ledger-technology/>

ABOUT RKVST

RKVST enables organizations to prove and verify the provenance and authenticity of any data they use in their business operations. Whether that's tracking nuclear material, underpinning climate transparency or eliminating supply chain disputes, RKVST provenance-as-a-service removes the frustration, time wasting and uncertainty of manual data verification.

Underpinned by blockchain technology, RKVST seamlessly integrates with existing software and secure data storage systems via an open API, creating a record of proof of origin, provenance and authenticity for any data. It's also then easy to share that provenance with partners, suppliers and customers, providing the transparency, integrity and trust that every business needs for its critical decision-making.

To learn more visit: www.rkvst.com