

EDM Webinar

One copy of the truth – Sir Tim Berners-Lee on Solid and the future of enterprise data

Live Date: July 14, 2026

Speakers:

- Moderator: **Emma Thwaites**, Strategic Advisor, Global Policy and Corporate Affairs, Open Data Institute
- **Sir Tim Berners-Lee**, Inventor of the World Wide Web, Co-founder/CTO, Inrupt Inc., Co-founder, Open Data Institute
- **John Bruce**, Co-founder and CEO, Inrupt Inc.
- **Jesse Wright**, Project Lead – Solid, Open Data Institute
- **Elisa Kendall**, Senior Ontologist, EDM Association
- **Jim Halcomb**, Chief Research & Development Officer, EDM Association

Presentation: [View slide deck](#)

Additional links:

- | | |
|---|---|
| <ul style="list-style-type: none">• Learn more about EDM Association• Create a profile on EDMConnect• Learn more about the DCAM and CDMC frameworks• Learn more about FIBO• EDM Association's Communities of Practice• FIBO on GitHub• Explore more EDMWebinars | <ul style="list-style-type: none">• Join the Solid Forum on EDMConnect – all are welcome!• Learn more about Inrupt• Meet Charlie• Learn more about Solid• More about ODI• Solid standard on GitHub |
|---|---|



WEBINAR Q&A:

Thank you to our panelists for providing the below answers to all questions posed during the live webinar. For more information or additional questions, [contact us](#) online, or email us:

Open Data Institute (ODI) and Solid: solid@theodi.org

Inrupt Inc.: support@inrupt.com

EDM Association: info@edmcouncil.org

Who owns the data, and where is it stored? What if I want to share my data for a fee? How would that work?

It is an open standard so many service providers implement Solids with different models. Very technical users can self host and have the data on their machine. Most people will store it in the cloud with a trusted pod host provider. It really depends on who you trust and your risk profile. Further, you will often see many physical storages under the hood so your financial data could still be stored with a trusted bank, your health data could still be physically stored with your GP or healthcare provider. This flexibility allows for the creation of new paradigms for data ownership, sharing, and even monetization. The specific arrangement would be determined by the individual use case, Solid provides a platform for more nuanced data ownership and use structures on the web.

That's a cool demo. Beyond the vision, Solid has struggled with adoption for 10 years now. Has anything changed? What is the plan?

Yes. We now have a W3C Working Group called Linked Web Storage making Solid a recommendation. There is also a surge in interest with the growth in GenAI - on multiple fronts: 1 it lets us build a lot of tools in the open source ecosystem much more quickly, 2 it fits well as the data storage layer for personal Agentic AI vision. Seen together these factors create a moment where Solid is more relevant, more legitimate, and easier to implement than ever.

Is the data in the pod editable by me? Also, how long will all those data points be stored, is there a fixed amount of time? Any other storage limitations?

Yes, the data in Pods are editable by users, in the same way that you can create, edit and delete documents on your computer. Solid as an open standard places no limitations around the time or size limits for data storage; providers of Solid pods will often put storage limits in place to prevent abuse of their services, or to tier usage.

EDM Association

One Liberty Plaza, 165 Broadway, 23rd Floor, New York, NY 10006 | info@edmcouncil.org | edmcouncil.org

Regarding POD data, are we in danger of creating an "echo chamber" so shared results just build on what we provide and not expand on what we may be interested in or be challenged rather than just based on our history?

This is entirely dependent on how people choose to build Apps, Websites and AI agents with Solid. I would say it is much less of a risk than the current web; for instance if we look at social media - people can have choice over recommendation algorithms; because they are not locked into the platform that they use for posting and viewing feeds. So I would argue that it is much more likely to reduce the echo chamber effect - and that is my hope for where the technology heads.

I love the fact that Solid POD keeps ALL this data, as presented by Jesse. Do we consider this data as the ORIGINAL, respected by ALL THOSE platforms which shared this data with my POD, or is the POD just a copy holder, like it is planned in the Flanders Solid Project?

Think of Solid as being able to store anything you store on your file system online, and Solid applications as analogous to desktop applications.

On your file system, a text file that contains your shopping list is the authoritative source of truth; and any app (e.g. your notes app) that you use to read that file clearly treats that as the source of truth for your shopping list.

You could also download a copy of a docusigned contract. In that instance, it is just a trusted copy of the contract that you can read in your PDF viewer.

Solid is exactly the same. For things like productivity apps (todo's, docs, your personal agent), the data in your Pod is going to be the source of truth which these apps collaboratively edit. Meanwhile, you can store a trusted copy of e.g., your drivers license in your Pod; but you are not going to be editing the document to change your date of birth.

What is Charlie? It has been mentioned many times.

Charlie is Inrupt's product building personal Agentic AI on top of Solid. You can find out more information at <https://www.inrupt.com/meet-charlie>.

Charlie is framed as solving the "chicken and egg" problem between applications and data. Can you say more about what that actually looks like for a developer building on Inrupt today?

When the "app" is a conversational AI interface, that technology's flexible and dynamic capability set (i.e. to chat usefully about almost any topic and ingest almost any type of data) is a perfect match for Solid's ability to store and share a flexible and dynamic spectrum of data from various parts of a user's life.

GenAI conversations also continuously generate a stream of user information from raw conversational logs and derived "memories," which are well suited to be stored in a Pod under user control. Essentially it becomes much easier to create compelling user experiences that quickly show the value of access to a

rich store of personal data, **and** to continuously augment that store of data with fresh information about the individual.

What value will my business/organisation get from implementing Solid?

What value did business get from the web? The universe of answers is too wide to capture in a few sentences, and is dependent on industry. Common areas of value include: a better 360-degree view of customers, safe & personal AI experiences, and consent-based data sharing with partner organisations.

With Solid, once I share my data with someone how are they stopped from downloading and keeping it?

Digital Rights Languages like ODRL (the Open Digital Rights Language), can be coupled with Solid to create contracts and legal accountability around data misuse. Automated compliance and auditing tools can also be deployed in implementations to create records of data shared along with conditions for that sharing (in ODRL or other form), which can serve as evidence of misuse, or breach of contract. The automated compliance tooling can help services maintain compliance with digital contracts. In short: there is no technical prevention of copying, but by systematising and conditioning sharing Solid can create clear evidence trails for enforcement of contracts and policies.

Where can I find and read the SOLID Standard?

The GitHub is available at <https://github.com/solid>, and there is more detail at <https://solidproject.org/>. The Open Data Institute are stewards of the standard.

Once you request to revoke access to your data for a certain organisation, how do we ensure that data is deleted on the other side? Will there be a technical solution that actually prevents them from copying the data in the first place? How does that work?

This is more about digital rights and legal recourse. Digital Rights Language like the Open Digital Rights Language are often used to make agreements that e.g. a service will only retain data for 6 months. If they are found to be storing it beyond that period then you would have grounds for legal recourse.

Is there any interaction/use or crossover between Solid and the At Protocol?

At the very least there is a crossover between individuals working on AT and Solid. Emelia Smith who used to work on Solid now works on the identity system for AT. So I expect identity / log in to be the first point where we align between the two.

As soon as I share my data via Solid Pod, I need to trust that my data is not stored elsewhere. So even if I revoke the access, how do I make sure the data is not distributed by the company to its 6743 Advertisement Partners?

No technology can guarantee that your personal data can never be misused under any circumstances by malicious actors. What Solid does in this circumstance is completely change the baseline understanding

between individual and company about how the individual's data can be used — and bring a new level of transparency for the benefit of the individual. Today, a company's right to share a user's data with advertising partners would be expressed in long, legally complex Terms & Conditions that a user must sign in totality in order to use the company's service. Then the user has no further visibility into what data is collected or how it's actually used, partially because the company would have no technically feasible way to keep them informed of this granular level of data usage. Solid provides the technical tools necessary for a user to share specific pieces of their data with a company or service for specific purposes, and to change that decision any time. If a company uses that data outside the intended purpose, they have broken the transparent agreement with the user. This moves the action into legally dangerous territory akin to deliberate data misuse, rather than today's business as usual.

How do we trust a POD provider?

Trust in a pod provider would have to be built the same way all other trust is built: through experience. This might look like new entities gaining people's trust through good work or auditable infrastructure (Solid's open nature allows for that), or could be shortcut if already trusted entities (like banks, governments, etc) were to step into this role.

Can you interrogate the semantics of data in the pod? For example, what's a record versus another kind of information, and the semantics of the subject matter (health, finance)?

That's part of what we want to work on in the EDMA [Solid Community of Practice](#), thanks for asking! We would, for example, reuse existing ontologies or develop new ones to support the semantics of the data folks might want to share.

Are there any incentives – other than doing the right thing of course – that would push companies to adopt SOLID? I think it's a great concept, just trying to understand if there is sufficient ROI for companies to give up owning your data as that is a powerful position these companies find themselves in.

Adopting Solid as an organization does not require "giving up" their data. There are many advantages to distributing Solid Pods to customers in a managed, governed way that balances the interests of both the organization and the individual. Common areas of value include: a better 360-degree view of customers, safe & personal AI experiences, and consent-based data sharing with partner organizations.

Does Solid use Blockchain? It would seem to me that for this to work it would have to be decentralized.

Solid and blockchain are different technologies that solve complementary problems. The primary goal of a blockchain is to get consensus on a (typically) public record. Such as the transaction history of bitcoin or ethereum. All nodes in a blockchain network will typically retain copies of this record.

In Solid, consumers pick a trusted host, or set of hosts, with whom they can store their data. Most consumers will pick a trusted host (e.g. a bank, or existing storage provider) to host their data. Users can upload whatever data and documents they like to this storage.

As someone who signed up for a solid community pod in 2018 only to lose access to my pod in 2020 when it shut down suddenly, what can you say about the robustness of the ecosystem now?

All free Pod services in 2018 were experimental environments for developer use only; and this should have been clearly marketed on the host page. That remains the case for most [hosted pod services](#) today; including [solidcommunity.net](#), which the ODI is now responsible for hosting.

One of the ODI's key focuses is to enable that market of Pod hosts and one of the goals of this community of practice is to support appropriate EDM members in becoming Pod hosts who can provide guarantees to customers of data persistence and portability.

How would you prevent people from sharing their data with bad actors?

When talking about Solid we often talk about Open Ecosystems where users can use their pod to interact with any Solid Application. This situation is analogous to the physical world, where people are free to associate with whomever they want, including malicious actors. That said, like in the real world, users could choose to rely on trusted third parties to help them discern good apps from bad ones - this could look like an additional, voluntary, data governance layer that signals known trustworthy actors, and warns users before they engage with bad actors (similar to dangerous website indicators seen in industry today). These services don't exist yet, but Solid's architecture as a web protocol layer would allow them to pop up when the need arises, either from new companies entering the market, or existing trusted firms in the space.

Alternatively, for early implementations, or sectors with strict data protection requirements on the pod provider, managed ecosystems could be considered. In this paradigm, pod providers keep an allow list of approved solid apps that can interact with the pods they serve. In this scenario, pod providers take on responsibility for setting up standards and processes for maintaining their allow lists. Inrupt has experience with these kinds of deployments through work with their enterprise customers.

One of the stated goals of the Solid Community of Practice is to create certifications within the Solid ecosystem. This will include certifications for Pod Providers, to provide consumers with confidence that their data is being securely. Certifications for application software - such as websites and mobile applications will also be developed, to enable consumers to discern which actors and software they can rely upon to manage information such as their financial and medical records.

This certification helps improve security in both open and managed ecosystems around Solid. In the open Solid ecosystem, consumers can refer to these certifications when deciding if they want to give an

application access to their Pod. In managed ecosystems the allow-lists can move from being curators that Pod providers manage - as is the case today - to being a list of certified applications that Pod providers defer to.

How does Solid control the data usage of services?

Yes there is a level of trust required once you have shared data with a service provider. With Solid there is a legal accountability layer that is often also used - you can use digital rights languages such as the Open Digital Rights Language (ODRL) to set an agreement with the organisation you are sharing the data with that says “you agree not to share data with third parties” and if they are found to you have legal grounds for recourse.

Are there any standard or best practices to share personal and non-personal data with AI Agents? I find having to share different versions of not very-well governed data is a major challenge. For example, even with different sessions of a ChatGPT/Claude/Gemini etc. platform, different versions of the truth can be provided. Solid can save the trouble of sharing different versions of the truth. How do you make sure Solid is the source of truth, instead of a biased observation?

Yes there is a standard way of managing data sharing with Agentic systems, including LLMs. Typically the types of data that are stored in Solid are structured records so it doesn't come with the kinds of biases that are built into probabilistic systems like LLMs.

Is there any documentation you can share on how it can be used with Brokerage data?

We've been working with a number of companies on use cases related to fund and brokerage information recently. There is a separate community at EDM Association – the [Data Management for Asset Managers \(DMAM\) forum](#) – that is developing use cases for that. In addition, within the new [FIBO Forum](#), the FIBO securities working group is adding more support for funds, mainly concepts for classifying pension funds at this time. In our ACTUS working group, we are also working to add the details needed to support ACTUS-based cash flow analysis.