

# Implementing Encrypted Private Data Sharing between Personal Data Vaults

Anushka Vidanage, Jess Moore, Dawei Chen, Tony Chen,  
Sergio José Rodríguez-Méndez, Graham Williams

1 May 2026

This work was partially funded by

- Australian Government's Medical Research Future Fund National Critical Infrastructure Initiative Grant MRFCRI000138
- Universities Australia and the German Academic Exchange Service (DAAD) grant 57701258
- Gurriny Yealamucka Health Services Aboriginal Corporation (GYHSAC) and Australian Government Department of Health grant GO-3133



Australian  
National  
University

Software  
Innovation  
Institute

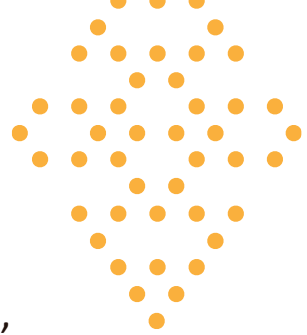
# About Us



Anushka Vidanage

Research Fellow

Research Interests – Data Privacy, Personal Online Datastores, Privacy Preserving Record Linkage (PPRL), Distributed ML



## Team



Prof. Graham Williams  
Chief Scientist



Jess Moore  
Chief Operating Officer



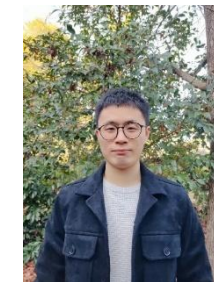
Dr Sergio Rodriguez Mendez  
Senior Research Fellow



Dr Dawei Chen  
Research Fellow



Yang Chen (Tony)  
Software Engineer

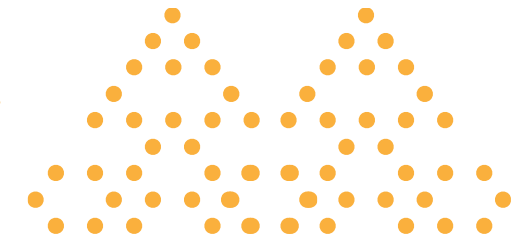


Zheyuan Xu  
Former Software Engineer



Ashley Tang  
Former Software Engineer

- Software Innovation Institute (SII) - <https://sii.anu.edu.au/>
- Solidcommunity AU website - <https://solidcommunity.au/>



# What Motivated Us

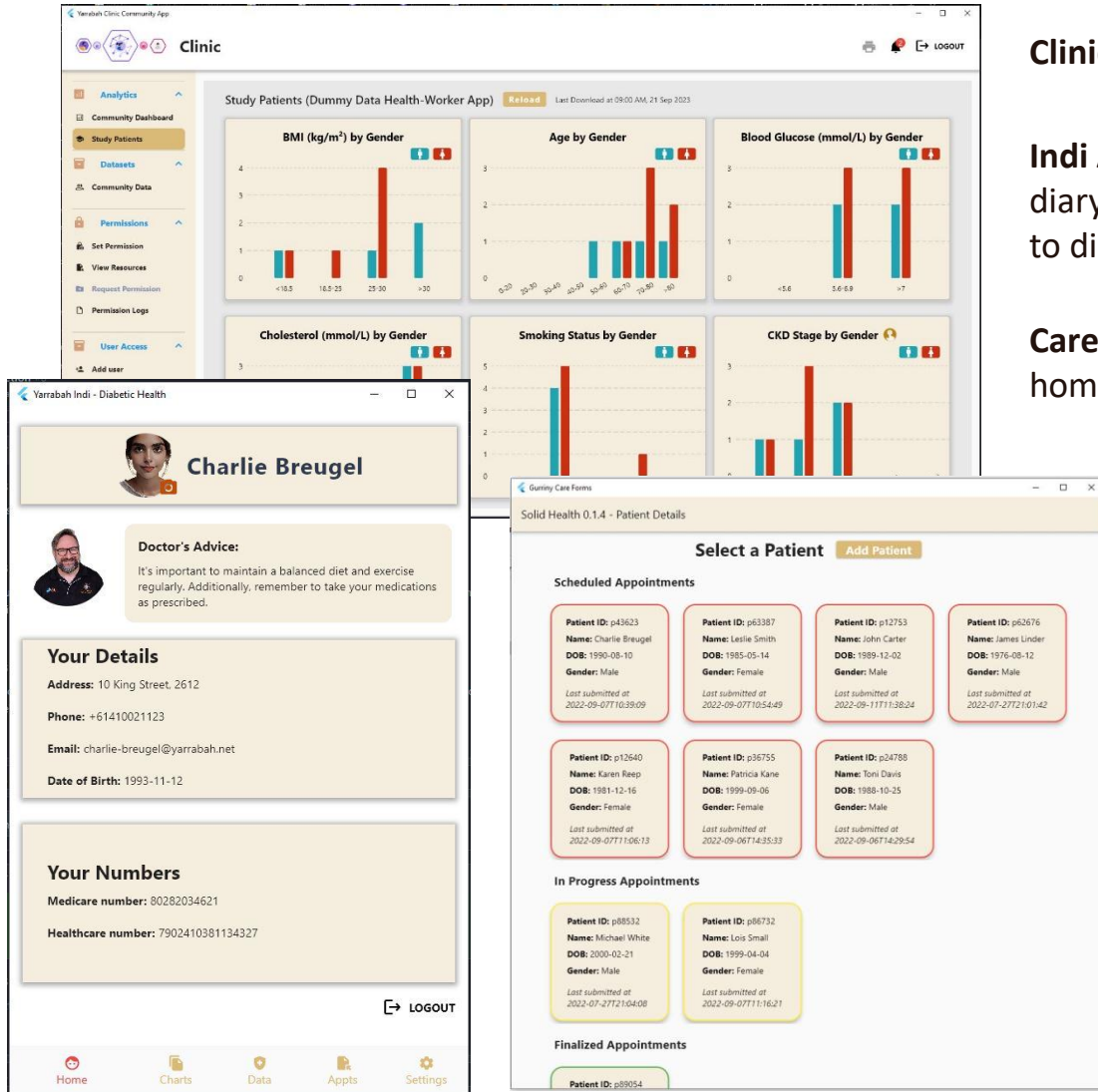


# Yarrabah

- ❖ Traditional country of the Gunggandji and Yidinji people. Mix of Traditional Owners and Historic Owners. Population of 4,500
- ❖ A project in collaboration with **Gurriny Yealamucka (Good Healing Water) health service** and Yarrabah leadership forum in Yarrabah
- ❖ Build a digital health platform to support integrated health care of Indigenous patients with diabetes using a person-centred data storage solution
  - ❖ We opted to use Solid Personal Online Datastores (PODs) to enable person centred solution



# Gurriny Indigenous Health Care



**Clinic App** to provide interface for doctors to analytics, insights, data for evaluation

**Indi App** to provide patients with diabetes info support tools from their GP, health diary to record well being, data access and control to support strength-based approach to diabetes management

**Care Coordination Team App** for patient record access and data collection during home care visits to patients

Challenge: Individuals must have control over their own medical and health data and be able to decide with who (doctors) they share their data

It is important for individuals in the indigenous community to know that they can have complete security and privacy of their data, and particularly their data in the cloud at rest

# Trust No One by Default



# Trust-No-One (TNO) environment

## ❖ Zero trust security model

❖ A privacy and a security architecture where a system does not automatically trust anyone or anything inside or outside its perimeters and instead must verify everything constantly - "never trust, always verify"

❖ *So, how do we ensure TNO environment in Solid PODs?*

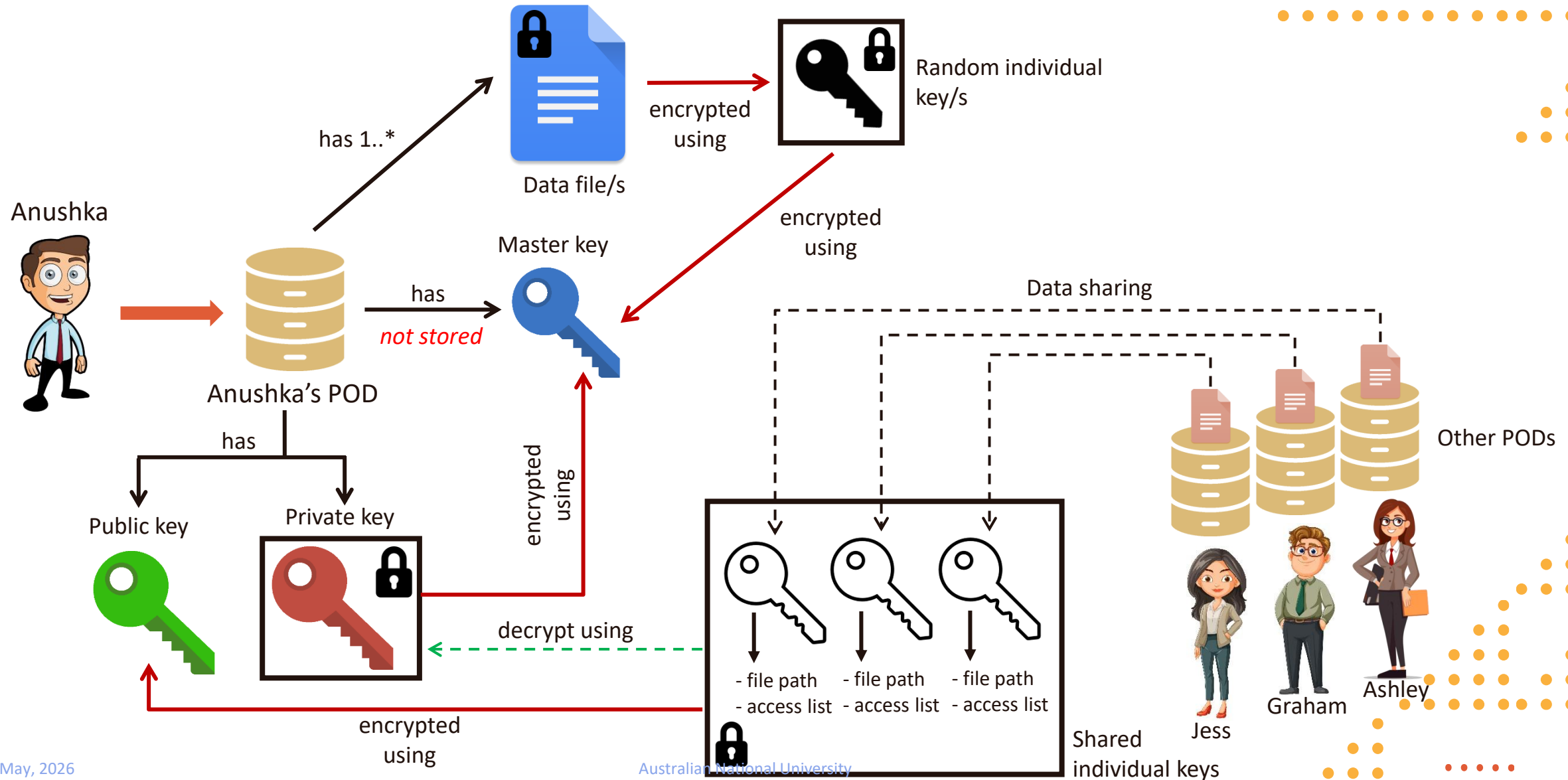
❖ *Data stored in PODs are encrypted by default*

❖ *Encrypted data are only ever decrypted locally on device*

❖ *The encryption keys are again encrypted using a master key*

❖ *Encrypted data are shared with others using public-key infrastructure along with Access Control Lists (ACLs)*

# TNO Architecture in PODs



# Secure POD Data Model (SPDM)

- ❖ Data model that captures the concepts and their relations regarding the system's TNO security model with main classes: Person, POD, DataFile, SharedKey

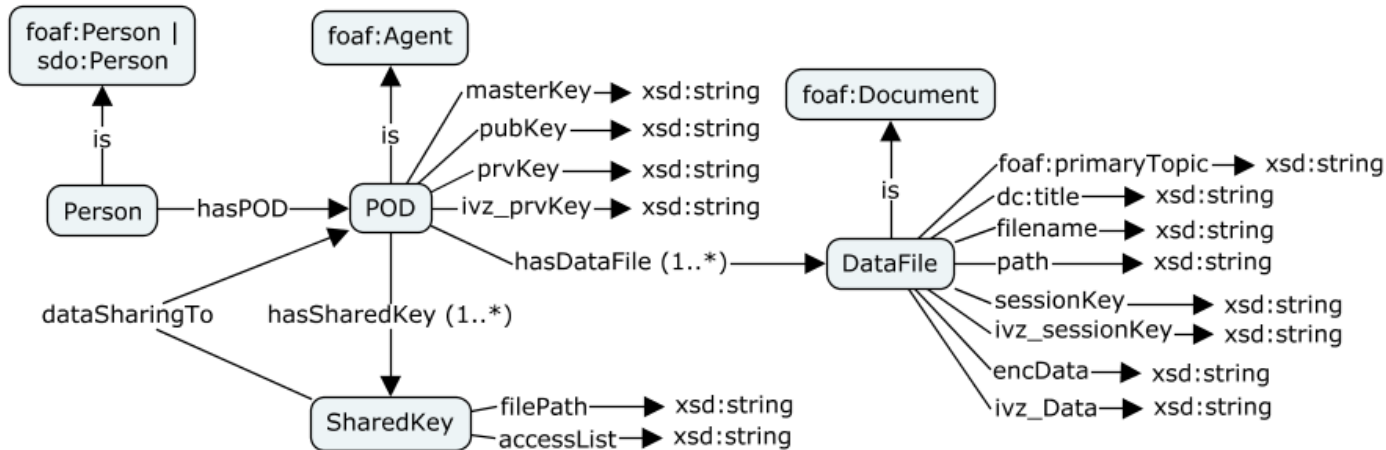
```

** EXTERNAL ONTOLOGIES & VOCABULARIES **
- foaf: <http://xmlns.com/foaf/0.1/>
- dc : <http://purl.org/dc/terms/>
- sdo : <http://schema.org/>
    
```

```

- "pubKey": public key.
- "prvKey": private key.

- "sessionKey": unique for each file (random symmetric key)
- "encData": encrypted data.
- "ivz_XXX": Initialisation vector value of the encryption algorithm for XXX.
    
```



# Current Work at SII in Solid PODs



# Rio: Closed Loop Non-Invasive Brain Stimulation Treatment

- Collects and analyse EEG data of project participants through a series of treatment sessions incorporated with brain stimulation



The image displays three overlapping screenshots of the Rio Pod software interface:

- Left Screenshot (User Profile):** Shows a 'Welcome to Rio Pod' message and a 'Profile Details' section for Participant ID: 7832, Name Initials: SS, Gender: Male, and Birthday: 07 Feb 1996. A status message indicates 'Your Pod is successfully linked with the trial!'. A 'Treatments Overview' section lists several active sessions, including 'Active Sham Mode Testing' and 'Testing new freq parameter'.
- Middle Screenshot (RIO Config Generator):** Shows the configuration for two channels, Channel S1 and Channel S2. Both are set to a 'Sine' waveform. Channel S1 parameters: Offset 0.0 mA, Sine Phase 1°, Sine Amplitude 1.2 mA, Sine Frequency 20.0 Hz. Channel S2 parameters: Offset 0.0 mA, Sine Phase 0°, Sine Amplitude 1.0 mA, Sine Frequency 50.0 Hz. Waveform graphs are visible for both channels.
- Right Screenshot (Participant Profile):** Shows a detailed profile for Participant ID 7832, Name SS, Gender Male, and DOB 07 Feb 1996. It includes a table of 'Enrolled Treatments' and a section for 'Completed Sessions'.

# User Driven Privacy

- ❖ Decentralised approaches such as PODs and federated learning shift privacy control to users, allowing them to decide how precisely their data is shared and in which amounts
- ❖ ***Can different privacy expectations from different users affect downstream machine learning (ML) performances?***
- ❖ Evaluated different data preparation methods (standard, granularity-based, and LLM-based imputation) against various data granularity to measure the performance changes. Tested with the following scenarios:
  - ❖ Anonymised training data
  - ❖ Anonymised inference data
  - ❖ Both anonymised
- ❖ **What we learned:** Effective learning under user-driven privacy does not require modifying ML models or reversing anonymisation. Instead, significant utility can be recovered by pre-processing anonymised data accordingly
  - ❖ Overall **specialisation** is the most robust and versatile strategy

Lange, L., Böttinger, A., Christen, V., Vidanage, A., Christen, P. and Rahm, E., 2026. Learning from Anonymized and Incomplete Tabular Data. *arXiv preprint arXiv:2602.01217*.











# The Ecosystem in Action

## ❖ Multiple Flutter/Dart based Solid packages for app development

- ❖ solidpod (<https://pub.dev/packages/solidpod>)
- ❖ solidui (<https://github.com/anusii/solidui>)
- ❖ solid-auth ([https://pub.dev/packages/solid\\_auth](https://pub.dev/packages/solid_auth))
- ❖ rdflib (<https://pub.dev/packages/rdflib>)

## ❖ Development of multiple apps based on Solid PODs

- ❖ Apps listed on solidproject web page <https://solidproject.org/apps>
- ❖ Also checkout our app directory at <https://solidcommunity.au/#portfolio>

 <b>InnerPod</b> A guided meditation timer that records each session to your Solid Pod with optional encryption. Built by the Software Innovation Institute, ANU. <a href="#">Source code on GitHub (lejewit/innerpod).</a>	 <b>MSFatigue</b> A survey/questionnaire app for multiple-sclerosis fatigue research; responses are saved encrypted to the participant's own Pod, with opt-in sharing to researchers. Built by the Software Innovation Institute, ANU. <a href="#">Source code on GitHub (anusii/msfatigue).</a>	 <b>FilePod</b> A Flutter-based Solid file browser — browse, upload, and download files on your Pod from any platform. Built by the Software Innovation Institute, ANU. <a href="#">Source code on GitHub (anusii/filepod).</a>
 <b>KeyPod</b> An encrypted key-value store usable as a password manager; also serves as a Flutter template for building Solid apps. Built by the Software Innovation Institute, ANU. <a href="#">Source code on GitHub (anusii/keypod).</a>	 <b>GeoPod</b> A map-based app for storing points of interest and tracks in your own encrypted Solid Pod. Built by the Software Innovation Institute, ANU. <a href="#">Source code on GitHub (lejewit/geopod).</a>	 <b>SecureDialog</b> A diabetes-logging app that stores entries encrypted in your Solid Pod. Built by the Software Innovation Institute, ANU.
 <b>TodoPod</b> An app to manage your tasks with all data securely and privately stored encrypted on your own personal online data store (Pod) hosted on a Solid Server. <a href="#">Built by Togaware. Source code on GitHub (lejewit/todoopod).</a>	 <b>RoloPod</b> A tool to collect your contacts into an address book in one secure and private place. You can selectively share any parts of your address book with others, or make phone calls on your mobile device (for the Android and iOS versions). <a href="#">Built by Togaware. Source code on GitHub (lejewit/rolopod).</a>	 <b>KonaPod</b> Collect your Hyundai vehicle data in one secure and private place. You can selectively share any parts of your data with others. The app presents the data and analyses of the data. <a href="#">Built by Togaware. Source code on GitHub (lejewit/konapod).</a>
 <b>BilliPod</b> Manage your bills, upcoming, scheduled, and past. The app analyses your bill history to generate reminders to avoid missing the all important bill payments. <a href="#">Built by Togaware. Source code on GitHub (lejewit/billipod).</a>		

# Thank you!

Appreciate your feedback!

Get in touch with us to know more about our work

Contact:

[graham.williams@anu.edu.au](mailto:graham.williams@anu.edu.au)

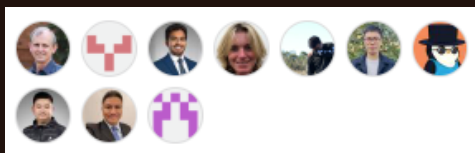
[anushka.vidanage@anu.edu.au](mailto:anushka.vidanage@anu.edu.au)

[SolidCommunity@togaware.com](mailto:SolidCommunity@togaware.com)

Where to start:

<https://github.com/anusii/solidui>

ANU Solid team



Explore further:

- <https://github.com/anusii/solidpod>
- <https://solidproject.au>
- <https://solidproject.org>

Get involved:

- <https://solidcommunity.au>
- <https://sii.anu.edu.au>