A DATABASE PER PERSON ON THE PLANET - A DEEPER DIVE ON SOLICT

Author: Guy Huntington, President, Huntington Venture Ltd,

Date: October 22, 2021

Table of Contents

Executive Summary

This document is aimed at the following types of architects:

- Legal
- Data
- Identity
- Security
- Network
- Etc.

It covers my thoughts on the following SOLICT components:

- Authoritative legal credential sources
- Toda
- SOLICT database per person
- Consent
- Authentication
- Authorization
- Session Assurance
- Special cases
- Legal agreements
- Global standards
- Global, independent, non-profit
- PIAM (personal identity access management) to manage consent, legal agreements and access management
- Token server?
- Updating SOLICT system
- Archival & data recovery policies
- Security architecture

Introduction

A prior LinkedIn document introduced an out of the box idea - give each person on the planet their own database containing their source of legal identity and credential truth (SOLICT). This paper begins to dive deeper into the weeds, containing my thoughts on components, questions, etc. It's NOT a quick read, as there's much to chat about. It's aimed at legal, database, identity, security, network architects, etc. It's also published on LinkedIn.

NOTE: This document used the term "PERSON" to indicate the actual person whom the SOLICT data is about. It also uses the term "MANAGER" for a person who is legally delegated to manage a PERSON'S SOLICT data, e.g. a parent/legal guardian, etc.

Components

- Authoritative legal credential sources
- Toda
- SOLICT database per person
- Consent
- Authentication
- Authorization
- Session Assurance
- Special cases
- Legal agreements
- Global standards
- Global, independent, non-profit
- PIAM (personal identity access management) to manage consent, legal agreements and access management
- Token server?
- Updating SOLICT system
- Archival & data recovery policies
- Security architecture

Authoritative Legal Credential Sources

Issue's legal identity, credentials, changes to them. Examples include:

- Rethought CRVS (civil registration vital statistics) system which also obtains forensic biometrics, e.g. fingerprints and iris
- School/post-secondary credentials
- Health credentials, e.g. Covid vaccinations
- Has a verifiable digital signature approved by the global, independent, non-profit
- Exports legal identity/credentials to SOLICT using global standards via Toda

Reference link: Skim pages 89-92 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Authoritative Legal Credential Sources - Relationships

Legal identity MUST be able to show legal identity relationships between different legal parties. Examples include:

- Parent/child
- Legal guardian/child
- Marriage partners
- Power of attorney/person
- Executor of estate/deceased identity

This will be done by the authoritative source cryptographically cross-linking different people's SOLICT data. So Jane Doe and her son John Doe's SOLICT data would be cryptographically cross-linked to each other showing a parent/child relationship. This is the tool to establish a PERSON/MANAGER LEGAL RELATIONSHIP

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Authoritative Legal Credential Sources – Authorization Rights

Authorization rights for managing consent per database attribute will be done via export Toda capability files (i.e., I'm not sure of the actual database architecture for this). For example, the local authority would write a capability file to Jane and John Doe's SOLICT giving Jane control over managing John's legal identity and credentials.

- These will be set by the global, independent non-profit

The person might have the capability of delegating some of their authorization rights to others. Hypothetically, Jane Doe might delegate some of her management rights of John Doe, to her parents for 3 weeks while she's away. This allows his grandparents the ability to control what identity data is released when he's in an AI/AR/VR environment at their place, as well as being able to legally prove his identity if he's taken to a hospital.

HOWEVER, note this becomes a slippery slope. I can easily see criminals leveraging this to obtain control over a person say in the sex trade. Thus, very careful thought must be given to this before implementation.

Capability files will be to global standards. I feel the capability files will be widely adopted because it's now out of each enterprise's control, i.e. they'll need it to determine what to do with consent from each person regarding their legal identity, data and credential use.

Who will be the standards body for the capability files? I'm not sure. Do we use something like Oauth or create something else?

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Authoritative Legal Credential Sources – What's Not Included

- Actual micro data about a person – Examples include:
  - Education data, e.g. Digital Learning Twin (DLT)
  - Health data
  - Etc.
- These may be contained within the person's citizen identity vault and/or distributed
- These other data sources might or might not be in control of the person (see SOLICT section of this document)

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

TODA

- Used by authoritative source to securely, send legal identity/credential information to the SOLICT
- Able to prove the data was sent (hash of the file) on a certain data and time to the SOLICT endpoint without duplication to other databases
- Used by PERSON/MANAGER of SOLICT to agree to consents to use data within SOLICT
- Potentially used by third parties to provide their consent to SOLICT in conjunction with Kantara's UMA - hypothetically, leveraging TODA with UMA makes some sense since Toda can prove the consent was sent from the third party to SOLICT on a certain data and time - this needs to be fleshed out and either adopted or not

Reference Link: 'Legal Identity & TODA"

SOLICT

- Database per person
- Stored in a global cloud outside a jurisdiction's control
- SOLICT IS NOT OWNED BY THE PERSON i.e. it's the legal identity and credential source for a person's identity
- HOWEVER, A person is the manager of their SOLICT data
- Mostly, the person is in control of their SOLICT data
- Exceptions to this include children, people requiring power of attorney, etc.
- Edge use cases need to be created defining exceptions -this is potentially a slippery slope as malicious people might want to use these to control a person's legal identity and credentials

SOLICT - What's Not Included

- Micro databases, e.g.:
  - Health
  - Education
  - Etc.
- I feel these are potential mine fields politically, commercially, etc.
- The person may or may not control these, e.g. they may delegate their rights to others willingly, or out of ignorance
- My thoughts - keep the scope tight for SOLICT and don't try to solve the planet's data privacy problems

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

SOLICT Database Design

Architecture for the actual database will likely be quite simple, i.e. global agreed attributes per person, consent, contracts, etc. However, perhaps a database architect will disagree with me, i.e. it all needs to be worked out by experts.

Assumptions:

- The data can only be written and never deleted
- Database can never be deleted
- Only archived
- Ability for a jurisdiction to change attributes
- How will the changes be noted?
- Use cases need to be created for “edge cases”, e.g. fake identity, malicious jurisdiction trying to alter an attribute about a person, etc.

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

SOLICT Database Architecture Policies

- Authentication policy for authoritative source to write to the database
- Authorization policies for the following:
- Authoritative source
- Consent manager
- Third parties consuming the information agreed to by the consent manager
- Others?
- Archival/storage policies
- Legal contracts/policies (see legal section)
- Others?

SOLICT - Security

- See last section of this document

SOLICT - Legal Agreements

- **This is the most important component piece**
- Need LOTS of legal expertise/help here understanding the scope of this, as well as driving out the details/deliverables, etc., i.e. there will likely be lots of detail for this
- The legal contracts spell out the function and policies of SOLICT
- IT MUST BE ABLE TO LEGALLY FUNCTION PAN-JURISDICTIONS AROUND THE PLANET

- Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Consent

There are five forms of consent:

- Authoritative source who's writing the data to SOLICT
- Third party wanting to access a piece of data within SOLICT
- "PERSON" who SOLICT is about
- "MANAGER" of SOLICT on behalf of "PERSON"
- Legal ruling requiring access to SOLICT data

Consent - Authoritative Source

- What consent mechanism(s) need to be in place for an authoritative source to write to SOLICT?
- How will this actually work?
- Use cases need to be developed
- It should start off with the CRVS creating SOLICT from birth
- All consents, and any writing to the database, MUST be recorded within SOLICT
- Other?

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Consent - Third Party Accessing SOLICT Data

- The actual consent mechanism should likely be some form of Kantara User Managed Access (UMA) - this may or may not be required to be modified
- A dumb question: If say Acme Inc. is granted access to Jane Doe's legal identity name, what needs to be included in the consent from Jane/SOLICT manager to Acme regarding Acme's authentication/authorization rights to then query the database and obtain her legal identity name?
- How will this actually occur?
- Other?

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Consent - "PERSON" Who SOLICT is About

- Assumption: Assuming the person is of legal age, then they won't require consent to access their SOLICT data to view it
- Is this assumption correct or not?
- See authorization section for more questions of viewing data
- Any time "Person" accesses SOLICT, their access MUST be recorded in the consent file within SOLICT i.e. its self-consent - is this assumption correct or not?
- How will the "Person's" PIAM play in all of this? - see PIAM section of this deck
- Other?

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Consent – "MANAGER" of SOLICT on Behalf of "PERSON"

- Assumption: MANAGER won't require consent to access their SOLICT data to view it - is this assumption correct or not?
- See authorization section for more questions of viewing data
- Any time "MANAGER" accesses SOLICT, their access MUST be recorded in the consent file within SOLICT i.e. its self-consent - is this assumption correct or not?
- How will the "MANAGER'S" PIAM play in all of this? - see PIAM section of this deck
- Other?

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Consent – Legal Ruling Requiring Access to SOLICT Data

- Use cases MUST be created addressing this
- This is the edge of a potentially very slippery slope as malicious states and criminals will likely try to use this to access “PERSON’s” data
- Assuming these use cases are valid, then what type of legal consent is required to then access ”PERSON’s” data, how should it be recorded in the consent file and how is this consent used to then authenticate and authorize the court to obtain the data they have specified?
- Other?

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Authentication

There are five entity types requiring authentication:

- Authoritative source who’s writing the data to SOLICT
- Third party wanting to access a piece of data within SOLICT
- "PERSON” who SOLICT is about
- “MANAGER” of SOLICT on behalf of “PERSON”
- Legal ruling requiring access to SOLICT data

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Authentication - Authoritative Source

- What is the credential assurance level required for the authoritative source’s system to authenticate to SOLICT?
- Will there be different credential assurance levels required for different types of authoritative sources based on risk? - e.g. a CRVS writing a legal identity might have a different risk level than say a high school writing a graduation credential to SOLICT
- All authentication events should be recorded somewhere in the SOLICT database

Authentication – Third Party Accessing SOLICT Data

- Based on the dumb question asked in consent, if say Acme Inc. is granted access to Jane Doe's legal identity name, what needs to be included in the consent from Jane/SOLICT "Manager" to Acme regarding Acme's authentication rights to then query the database and obtain her legal identity name?
- How will this actually occur?
- Will there be different levels of credential assurance for different types of access to SOLICT? - e.g. A request to prove Jane's a human is potentially at a different credential risk level that if they want to obtain her forensic biometrics
- All authentication events should be recorded somewhere in the SOLICT database
- Other?

Authentication – "PERSON" Who SOLICT is About

- What type of credential assurance should be used for "PERSON"?
- Should there be stronger credential assurance for accessing different portions of SOLICT by "PERSON"? - e.g. If Jane wants to view all her consents given from birth to date, is the risk higher or not than viewing her school credentials?
- All authentication events should be recorded somewhere in the SOLICT database
- How will the "PERSON's" PIAM play in all of this? - see PIAM section of this document
- Other?

Authentication – "MANAGER" of SOLICT on Behalf of "Person"

- What type of credential assurance should be used for "MANAGER"?
- Should there be stronger credential assurance for accessing different portions of SOLICT by "MANAGER"? - e.g. If Manager wants to view all consents given for Jane from birth to date, is the risk higher or not than viewing her school credentials?
- All authentication events should be recorded somewhere in the SOLICT database
- How will the "MANAGER's" PIAM play in all of this? - See PIAM section of this document
- Other?

Authentication – Court Requiring Access to SOLICT Data

- How will the consent be used to then authenticate the court's system or their appointee to obtain the data they have specified?
- As per the above types of entities, are their different credential assurance levels required to access different portions of "Person's" SOLICT?
- All authentication events should be recorded somewhere in the SOLICT
- Other?

Authorization

There are five entity types requiring authorization:

- Authoritative source who's writing the data to SOLICT
- Third party wanting to access a piece of data within SOLICT
- "Person" who SOLICT is about
- "Manager" of SOLICT on behalf of "Person"
- Legal ruling requiring access to SOLICT data

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Authorization - Authoritative Source

- What is the authorization policy required for the authoritative source's system to authorize to SOLICT?
- All authorization events should be recorded somewhere in SOLICT database
- Other?

Authorization – Third Party Accessing SOLICT Data

- Based on the dumb question asked in consent, if say Acme Inc. is granted access to Jane Doe's legal identity name, what needs to be included in the consent from Jane/SOLICT "Manager" to Acme regarding Acme's authorization rights to then query the database and obtain her legal identity name?
- How will this actually occur?
- All authorization events should be recorded somewhere in SOLICT database
- Other?

Authorization – "PERSON" Who SOLICT is About

- What type of authorization policies should be used for "PERSON"?
- All authorization events should be recorded somewhere in SOLICT database
- How will the "PERSONs" PIAM play in all of this? - see PIAM section of this document
- Other?

Authorization – "MANAGER" of SOLICT on behalf of "PERSON"

- What type of authorization policies should be used for "MANAGER"?
- All authorization events should be recorded somewhere in SOLICT database
- How will the "MANAGER's" PIAM play in all of this? - see PIAM section of this deck
- Other?

Authorization – Court Requiring Access to SOLICT data

- How will the consent be used to then authorize the court's system or their appointee to obtain the data they have specified?
- All authorization events should be recorded somewhere in SOLICT database
- Other?

Session Assurance

Based on the answers to the credential and authorization policies already asked then, during a session, the credential and/or identity risks might require increased stronger levels of identity and/or credential assurance

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Special Cases

- There are always exceptions in life requiring special cases
- Examples include leaders of countries, spies, people being sheltered by a government, .e. witness relocation program, etc.
- These are edge cases which also are the beginning of a slippery slope for criminals/malicious states will try to leverage these to do potentially bad things
- Use cases MUST be created and then very careful thought given to them
- **If you make an exception once, it can be reused over and over as justification for other people/entities**

Reference link: Skim pages 93-110 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Standards

Without standards, SOLICT won't be able to exist and function around the planet. SOLICT will likely use or create the following global standards:

- New CRVS data standards for legal identity
- HL7 type standards for health credentials - I'm not sure what Covid vaccination credentials are
- Education credentials for secondary/post secondary - These need to be created
- Trades/professional standards - These need to be researched and, if no global standards exists, create them
- Kantara User Managed Access (UMA)
- TODA
- Capability authorization files
- Legal consent contracts
- etc.

Reference link: Skim pages 89-92 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Standards - Global Bodies

- Wherever possible, SOLICT should leverage existing standards bodies - e.g. Health, professional bodies, etc.
- HOWEVER, the global standards bodies must be prepared to rapidly adjust them based on new attack vectors created by this curve - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf .
- As the global, independent, non-profit identifies very high risk attack vectors affecting the global standards, their transmission to SOLICT, etc. then the global bodies MUST be prepared to readily change standards, business processes, etc. as per the threat levels.

Global, Independent Non-Profit

- It's the gatekeeper for both Toda LSSI and SOLICT
- Thus, at an operational level, it's the most important operational piece
- It oversees:
  - Standards
  - 24x7x365 threat analysis against legal identity/credential governance, business processes, tech and end users
  - Security and fixes
  - It manages the politics associated with Toda LSSI and SOLICT
- Since it's planetary, relying upon each jurisdiction to comply, this is also one of the main critical components of SOLICT

Reference link: Skim pages 143-155 "Cost Centre - Rethinking Legal Identity & Learning Vision"

Global, Independent Non-Profit Suggested Scope

- Oversees coordination of global standards bodies responsible for legal identity and credential standards
- Coordination means the following:
- Inserting themselves into the change management lifecycle for applicable standards such that any potential change affecting SOLICT is notified and well tested out in advance
- Inserting themselves into emergency change processes
- This will likely be created by the non-profit identifying very high risks for a specific standard requiring emergency fix processes
- The goal is to have a seamless process for both the responsible standards body and the non-profit re SOLICT
- It might or might not be responsible for the following standards:

- CRVS legal identity
- PIAM (Personal identity access management)

Other scope activities:

- Does 24x7x365 threat analysis against the legal identity and credentials used in SOLICT and a PERSON's Toda LSSI
- Produces threat analysis
- Monitors changes made as a result of the threat analysis and fix recommendations implemented
- Oversees implementation of standards and fixes to Toda LSSI and SOLICT databases
- Other?

Global Independent Non-Profit Governance

Very careful thought need to be taken when considering who governs the non-profit. I suggest a mix of the following:

- Some global standards bodies
- A representative from legal law societies
- A representative from a privacy body
- Other?

I also suggest voting require 2/3 majority to make a major change on the board. This prevents rapid changes in board management.

Finally, I also suggest a group of independent auditors be required to independently audit the non-profit to ensure it's "squeaky clean".

Global Independent Non-Profit Funding

- Governments pay a fee for use of the new age CRVS system plus also enabling LSSI up to a maximum amount per year
- Addressing this is one of the most important components of the SOLICT puzzle
- If the amount of money raised is too small, it will result in the non-profit cutting corners, and likely lead to weak overall security, i.e. it could prove fatal to billions of SOLICT databases around the planet
- Other?

Reference link: Skim pages 151-153 "Cost Centre - Rethinking Legal Identity & Learning Vision"

PIAM (Personal Identity Access Management) System

PIAM, leveraging AI will be used to conduct:

- Consent agreements/legal contracts on the fly between “PERSON” or her “MANAGER” and third parties wanting to access “PERSON’s” SOLICT data
- Access management with the SOLICT and third parties
- Access management with “PERSON” accessing their SOLICT
- Access management with “MANAGER” accessing “PERSON’s” SOLICT

Some dumb questions about PERSON/MANAGER’s PIAM and SOLICT:

- What role does the PIAM have regarding IAM management of SOLICT?
- What security and access monitoring systems are installed with PERSON’s SOLICT?
- Does PIAM play a role in this?

PIAM requires standards to ensure all PIAM’s are securely, accessing and controlling access to PERSON’s SOLICT. I see the global, independent non-profit driving this, at least to start with.

Reference link: Skim pages 127-134 "Cost Centres - Rethinking Legal Identity & Learning Vision"

Database Tokenization?

Dumb questions:

- Does the SOLICT database Token-ize it's data? - This can mitigate risk of the SOLICT being hacked and the data being exposed
- How will this work with the potentially hundred of requests as "PERSON" walks down a street, creating contracts on the fly, via "PERSON's" PIAM, for releasing consent to various this parties? -Or, does it not work?
- If it does work, then the architecture must have a external facing database containing token data, with behind it the token server
- All of this needs to be very carefully thought out and architected for from a security perspective
- Other?

Reference link: Skim pages 93-110 "Cost Centres - Rethinking Legal Identity & Learning Vision"

System Upgrades

Dumb questions:

- How will underlying system components be securely updated? - e.g. firewalls, endpoints, database, etc.
- How will this be automated?
- What will be hotfix update processes?
- Consider the scale in the not so distant future and reflect on implications, e.g. billions of people's SOLICT databases might require hotfix upgrades within hours
- Other?

Reference link: Skim pages 93-110 "Cost Centres - Rethinking Legal Identity & Learning Vision"

Archival & Data Recovery Policies

- What happens to PERSON's SOLICT when they die?
- What conditions have to be required to archive a SOLICT database?
- What are the archival policies?
- What are retrieval policies if and when a SOLICT database has to be retrieved?
- All of this is VERY legal and must be well thought through
- As well, it's also has costs, technical and security implications
- Other?

Reference link: Skim pages 93-110 "Cost Centres - Rethinking Legal Identity & Learning Vision"

Security Architecture

All of the previous sections above affect the end-to-end security architecture for SOLICT, which is why I've put this at the end of the deck. Security attack vectors include:

- Tech used
- Governance
- Business processes
- End user

All of the above MUST be fleshed out. It's a moving target due to this curve - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf .Thus, today's best security architecture might be tomorrow's turd.

SOLICT IS ALL ABOUT TRUST. So, the security architecture has to be "damned good" and continually "damned good". As I see it, this is a very big challenge.

Reference link: Skim pages 93-110 "Cost Centres - Rethinking Legal Identity & Learning Vision"

Summary

This document is my first attempt to think my way through the requirements to design, build, implement and maintain a SOLICT system. It's out of the box thinking, which requires out of the box solutions. Thus, I welcome all comments, thoughts, criticisms and suggestions.

About Guy Huntington

I do short term consulting for Boards, C-suites and Governments, assisting them in readying themselves for LSSI (legal self-sovereign identity). I;ve written over 30 papers about this from the bedroom to the boardroom (https://hvl.net/pdf/Who%20am%20I%20identity%20verification%20papers%20summary%20Mar%202019.pdf)., as well as numerous LinkedIn articles (https://www.linkedin.com/today/author/ghuntington).