Antitrust Policy & Member Participation

Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws.*

Only members of Trust over IP who have signed the necessary agreements and charters are permitted to participate in this activity beyond an observer role.

* Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy.
Agenda

› Possible Remarks Executive Director, John Jordan - 3 min
› Announcements - 5-10 min
  › New ToIP Website has launched
  › New Members Orientation next Friday, August 27th 9am PT
  › Storage and Portability Task Force - Speaker September 13th
  › Guardianship Addendum Task Force - Call for Action
› Today’s Special Topic - Trust Registries (30 min)
› Open Q & A (All) - 10 min
Dr. Peter Wittenburg

FAIR Digital Objects – self-standing data entities for organising our digital data space

Speaking at storage and portability TF
Monday September 13th
9am PDT/12pm EDT/4pm UTC/6pm CEST

Dr. Peter Wittenburg is highly esteemed in the research data community and is currently engaged in significant developments around research data. This includes his leading roles in building European research/data infrastructures (CLARIN, EUDAT), in the Research Data Alliance and in contributing to the launch of the multi-billion Euro European Open Science Cloud (EOSC).
Guardianship:
The Need for the GHP Blueprint to Consider Guardianship

Presented by the Chairs of the Guardianship Addendum
John Phillips and Jo Spencer
August 2021
The Good Health Pass Blueprint is a great initial achievement.

Version 1.0.0 of the Blueprint has constructed a holistic approach to travel enablement using credentials that can be verified and trusted.
The current release focuses on self-directed travellers.

Assumptions are that the traveller is able to register themselves.

Travellers hold their own identity, health and pass credentials.

Digital models and digitally enabled physical models (and a mix) are supported.

Verification is through the presentation of credentials by each traveller, individually.
As travel begins post-pandemic, families will be a large proportion of travellers.

Familiarity with remote working and time lost to quarantine means that business travel will reduce.

Many families have an intense need to reconnect.

Unaccompanied or dependent travellers will need to be supported.

Digitally supported travel needs better proof of guardianship relationships.
Guardianship concepts to be added to the blueprint.

Pass management must be possible on behalf of / for dependents.

Unaccompanied minors need passes and trusted destination pick up.

Dependent adults and seniors should be supported too.

Guardianship credentials can provide a way to do this.

Family, and unaccompanied and supported travel demand a specific approach.
Approaches we identified in the Sovrin Guardianship Working Group are directly applicable to Travel Passes and guardian activities.

Jurisdictions need to be catered for such that they can evolve and control travel independently.

The mental model helps the definition and use of VCs.

There are a few references in the GHP blueprint that make guardianship solution assumptions.
We have a framework that needs to be tested and the findings reflected into the Blueprint.
We need your help
We have developed a Guardianship Addendum for Blueprint 1.0.0

We will not be updating the whole of the document to consider guardianship.

An addendum (chapter) to be separate for this version.

Next versions of the blueprint may incorporate more guardianship considerations throughout.
We need to coordinate with the other authors, experts and groups

The insertion of guardianship credentials into each model needs consideration - physical, digital, mixed.

User interactions for pass registration need to change.

Trust registries and rules implications need to be understood.

Practical use of travel passes by guardian on behalf of a traveller.

What are the commercial model implications?
We need input from the other drafting groups and external experts.
Addendum Drafting Group Activities and timelines

Twice weekly discussions:

› Monday 1600 PST, Tuesday 0900 AEST
› Thursday 0930 CEST, 1730 AEST

Zoom meetings on TOIP Calendar.
ToIP Slack channel #ghp-guardianship

Wiki page:
https://wiki.trustoverip.org/display/HOME/Guardianship

Aim: Final Addendum Draft for completion by end-Sept
What do you think?

We’re listening...
Special Topic - Trust Registries

- **Trust Registry TF co-chair Darrell O'Donnell**
  will introduce the overall concept of trust registries and the special role they play in ToIP architecture.

- **Trust Registry TF co-chair Drummond Reed**
  will explain the unique way in which trust registries integrate the two halves of the ToIP stack, i.e., bring together the technical “tools” with the governance “rules”.

- **Lucy Yang, Community Director of Covid Credentials Initiative (CCI) and staff at Linux Foundation Public Health (LFPH)**
  will explain the business reasons why trust registries are at the core of the LFPH's Global COVID Certificate Network (GCCN) project.

- **John Walker, Community Architect of CCI and staff at LFPH,**
  will explain how GCCN is tackling the task of offering a global directory of trust registries for COVID-19 certificates.
Special Topic: Trust Registries
Special Topic - Trust Registries

- Trust Registry TF co-chair Darrell O'Donnell will introduce the overall concept of trust registries and the special role they play in ToIP architecture.
Verifiable credential compliant with Good Health Pass policies

COVID-19 test admins
Certified testing devices
Primary care providers, labs, retail health
National health systems
Other health data exchanges

Government border systems
Airline departure control systems
Airport secure zone border systems
Airline boarding & advanced passenger systems

Governance Framework
Verifiable credential compliant with Good Health Pass policies

Listed In Trust Registry

Governance Authorities

Controls

Privacy-respecting credential proof

Uses

Trust Registry

People

Digital Wallet

Holders

Uses

Issuers

Verifiers

Travel

Governance Framework

Health

• COVID-19 test admins
• Certified testing devices
• Primary care providers, labs, retail health
• National health systems
• Other health data exchanges

• Government border systems
• Airline departure control systems
• Airport secure zone border systems
• Airline boarding & advanced passenger systems
CRITICAL INTERACTION - Presenting a GHP pass

Issuer

Holder

Verifier

Biz Logic / Rules Engine

GHP BBS+ health credential

GHP BBS+ health pass

Trust Registry API

Trust Registry

listed in
What Does a Trust Registry Do - EXTERNALLY?

Shares the key information that

- Issuers and Verifiers - aut
- Key DID information
  - EGF
- Key Ecosystem information - provide answers
  - What type(s) of credential(s) are in used?
  - What uses (presentations) of credentials are “normal” under the EGF?
  - What Layer 1 Utilities are supported?
- Initially the Trust Registry Task Force is focused on the most basic minimum use case.
Trust Registry Task Force

Initially the TRTF is focused on the External view of a Trust Registry

Minimum Viable API - aimed at implementers for Verification use case.
- CheckIssuer()
- CheckVerifier()
- CheckTrustRegistry()
- GetOffLineFile()

Future work will include more capabilities:
- Credential & Interaction Types
- Cryptographic information (e.g. point to KERI records)
Special Topic - Trust Registries

- **Trust Registry TF co-chair Drummond Reed**
  will explain the unique way in which trust registries integrate the two halves of the ToIP stack, i.e., bring together the technical “tools” with the governance “rules”.
Part Five:
Governance Frameworks and Trust Registries
To be both interoperable and trusted, the Good Health Pass digital trust ecosystem needs governance.

See Recommendation #9: Governance and Trust Frameworks and The Good Health Pass Ecosystem Governance Framework.
The role of a governing authority is to be responsible for developing, publishing, and maintaining a governance framework.

See Recommendation #9: Governance and Trust Frameworks and The Good Health Pass Ecosystem Governance Framework.
The governance trust diamond
To interoperate across trust boundaries, ecosystem members need to be able to quickly and securely verify who is authorized to do what—this is the role of a trust registry.

See Recommendation #8: Trust Registries
The trust registry maintains a list of all authorized issuers in its ecosystem and the types of credentials and passes they are authorized to issue.

See Recommendation #8: Trust Registries
A verifier can use the **issuer DID** and **type URI** embedded in every GHP-compliant credential to query the trust registry whether the issuer is authorized.

See Recommendation #8: Trust Registries
trust registry

rules

engine
governance

framework

credential

issuer

holder

pass
governing authority

governing authority

verifier

governing authority

queries to verify issuer
to

issues

registered in

registered in

controls

published rules

regulations & queries
to qualify holder

issues

queries
to

registered in

to

query

queries
to verify verifier

published rules

regulations & queries
to verify pass

to

published rules

regulations & queries

Some governance frameworks also require verifiers to be authorized—in this case, a holder can query the trust registry to “verify the verifier” before sharing any data.

See Recommendation #8: Trust Registries
trust registry

rules engine

governance framework

credential

issuer

pass

verifier

holder

queries to verify

issues to register

registered in

governing authority

rules & queries to qualify

trust registry

controls

publishes

registered in

publishes rules & queries to verify
Final note: another option for trust verification is **chained credentials**—where a governing authority issues a VC authorizing the issuer and the issuer chains it to the VCs issued to holders.

See Recommendation #8: Trust Registries
For more about credential chaining, see the Authentic Chained Data Container (ACDC) Task Force in the ToIP Technical Stack WG
Special Topic - Trust Registries

- Lucy Yang, Community Director of Covid Credentials Initiative (CCI) and staff at Linux Foundation Public Health (LFPH) will explain the business reasons why trust registries are at the core of the LFPH’s Global COVID Certificate Network (GCCN) project.
Global COVID Certificate Network

June, 2021
Global COVID Certificate Network (GCCN)

A Linux Foundation Public Health initiative to enable interoperable and trustworthy verification of COVID certificates between jurisdictions for safe border reopening.

GCCN will support Global COVID Certificates (GCC) that apply to three use cases: vaccination, recovery from infection, and test results.

We work with governments and industry alliances, software vendors and systems integrators, supporting organizations, and the broader LFPH community to jointly develop a trust registry network, a complete set of toolkit to build COVID certificate ecosystems and a vendor network for GCCN.
Current state of COVID certificates - EU leads the way

› EU recently set the pace for COVID certificates by launching the **EU Digital COVID Certificate**: the EU **Gateway** and the **national certificate systems** of Member States.

› This Gateway is a centralized repository for public keys, a system designed to be the root of trust between EU member states.

› This Gateway provides a flexible framework for member states to decide how to create their own trust registry of authorized issuers and verifiers while enabling them to verify certificates issued from other member states.

› The **EU eHealth Network provided guidelines** for the development of the Gateway and national certificate systems.
Challenges being brought up after the EU announcement

- There is a lack of a global trust architecture, a framework that enables verifiers in one jurisdiction to make a decision about whether or not to accept a certificate signed by another jurisdiction.
- Government policy makers and technology teams don't have enough clarity about how to build and manage COVID certificate systems.

Given these challenges, we asked:

- As a global organization building open source software for public health, what can we do to reopen borders in an interoperable and trustworthy manner?
LFPH created GCCN to address these challenges

1. Trust Registry Network - Interoperable Trust/Key Management
   - There is a way for the various trust registries in every jurisdiction to find each other and decide whether to accept each other’s certificates
   - There is a way to look up data on who is doing what, and a way to contact them
   - LFPH will facilitate the development of a trust registry protocol that allows everyone to talk to each other
   - LFPH will set up a lightweight initial governance and will facilitate entities in the network to self govern moving forward.
EU: Trust and interoperability through centralized key management

LFPH created GCCN to address these challenges

GCCN: decentralized key management and interoperable trust registry protocol
LFPH created GCCN to address these challenges

(2) A Complete Toolkit to Build Certificate Ecosystems - Interoperable & Privacy-Preserving Credential Verifications
   › Governance framework template.
   › Schema definitions and minimum datasets: vaccination, recovery, test results.
   › Technical specifications: credential formats and signing protocols, QR code specifications, certificate applications, etc.
   › Implementation guides and open source reference implementations
   › Implementation and governance guidance

(3) Vendor Network
   › We are building a directory of vendors who can competently work on these kinds of projects, so that governments and institutions can more easily get running.
GCCN builds off the GHP Blueprint Recommendations
GCCN next steps

› Technical Development
  - Work with communities to define the MVP for GCCN based on the GHP Blueprint and collaboratively develop the technical documents and codebases.

› EU Collaboration
  - Collaborate with relevant EU institutions to explore and create conversion mechanisms between the EU Digital COVID Certificate and new and existing COVID certificate ecosystems through GCCN.

› Interoperability Pilots
  - Get key existing implementers to set up interoperability among each other through GCCN.
How to get involved

To receive frequent updates on GCCN, sign up for email communication [here](#).

**Government agencies or industry alliances** that already running or are looking to launch a COVID certificate ecosystem for border reopening should reach out to us at [info@lfph.io](mailto:info@lfph.io).

**Implementers of existing COVID certificate ecosystems** focused on reopening borders can reach out to us at [info@lfph.io](mailto:info@lfph.io) and join our [Slack](https://join.slack.com?l=lfph) #gccn stay up-to-date and #cci to exchange experiences with other implementers.

**Developers** can contribute to the reference implementations by joining our [Slack](https://join.slack.com?l=lfph) #gccn and getting involved with LFPH’s two COVID credentials projects: [Cardea](#) and [Medcreds](#).
Special Topic - Trust Registries

- John Walker, Community Architect of CCI and staff at LFPH, will explain how GCCN is tackling the task of offering a global directory of trust registries for COVID-19 certificates.
Global COVID Certificate Network (GCCN)

Trust Registry Network Starting Definition

The GCCN Trust Registry Network is an online resource that provides human and machine readable information pertaining to its network entries (participants). Network participants consist of public and private sector entities providing the issuance and/or verification of digital or digitized paper Certificates, Credentials or Passes required for use by jurisdictions to allow free and safe movement within or across locales.

The GCCN Trust Registry Network participants will provide users with qualitative information regarding the validity of any network entry

a. Network participant onboarding
b. Out of band - KYC, GCCN governance vetting
c. Human and machine readable attributed definitions
d. Support pre-operational discovery lookup of ‘who should I trust?’
e. Qualitative description of each entity listed
GCCN Trust Registry Network Proposed Profile

a. A named established entity
   i. Physical and Digital points of contact
   ii. Named entity operating the entry ‘network’
   iii. List / Definition of trust roles supported
   iv. Relevant industry classifications or certifications of entry

b. Operating model for the entry - self described

c. A description / qualification of the onboarding and vetting processes

d. Governance
   i. Named governing entity(s)
   ii. Link to governance ‘document’
   iii. Qualitative evaluation of
   iv. Machine readable to governance framework link

e. Security Profile / Compliance
f. Network / Geographic footprint

g. Types of identifiers / certification supported:
   PKD | DID | Signed credential
      i. Issuance and Revocation capabilities

h. Service Endpoint(s)
   i. Registration
   iii. Query API endpoint

i. GCCN status
   iv. GCCN KYC vetted
   v. Operating status
   vi. Operating dates
# The GCCN Trust Registry Network - Candidate Directory Entries

<table>
<thead>
<tr>
<th>Trust Entity</th>
<th>Type</th>
<th>Trust Roles Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCCN Trust Registry Network</td>
<td>A directory of trust networks</td>
<td>Meta</td>
</tr>
<tr>
<td>CommonTrustNetwork</td>
<td>A network of issuers and verifiers - common verification format</td>
<td>Issuer / Verifier App</td>
</tr>
<tr>
<td>New York State</td>
<td>A jurisdictional authority listing Issuers and providing a verification format</td>
<td>Issuer / Verifier App</td>
</tr>
<tr>
<td>EU eHealth Gateway</td>
<td>A directory of legally bound issuers and verifiers</td>
<td>Meta / Issuer / Verifier App</td>
</tr>
<tr>
<td>AOKPass</td>
<td>A network of issuers and verifiers - common verification format</td>
<td>Issuer / Verifier App</td>
</tr>
<tr>
<td>State of California</td>
<td>A jurisdictional authority listing Issuers and providing a verification format</td>
<td>Issuer / Verifier App</td>
</tr>
<tr>
<td>IATA</td>
<td>A network of issuers and verifiers - common verification format</td>
<td>Issuer / Verifier App</td>
</tr>
<tr>
<td>Walmart</td>
<td>A commercial / professional reference registry</td>
<td>Issuer / Verifier App</td>
</tr>
</tbody>
</table>
# GCCN Trust Registry Network Attribute Definition

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Entry Identifier</td>
<td>Unique ID</td>
<td></td>
</tr>
<tr>
<td>Entity Name</td>
<td>String</td>
<td>Entity’s provided legal name representation</td>
</tr>
<tr>
<td>GCCN Status</td>
<td>Active / Not Active</td>
<td></td>
</tr>
<tr>
<td>GCCN KYC Confirmed</td>
<td>Yes / No</td>
<td>Out of band process to be defined</td>
</tr>
<tr>
<td>Level of Assurance</td>
<td>(eiDAS)</td>
<td></td>
</tr>
<tr>
<td>Legal Entity Identifiers</td>
<td>[ Array of entries ]</td>
<td>GLEIF , other</td>
</tr>
<tr>
<td>Root of trust URI</td>
<td>string</td>
<td>X.509 or DID</td>
</tr>
<tr>
<td>Trust Type</td>
<td>X.509 / DID / other</td>
<td></td>
</tr>
<tr>
<td>Service Endpoint</td>
<td>DID / URI / URL</td>
<td></td>
</tr>
<tr>
<td>Ecosystem Governance URI</td>
<td>URI / URL</td>
<td>Link to ecosystem governance</td>
</tr>
<tr>
<td>Governance Framework</td>
<td>URI / URL</td>
<td>Link to entity’s gov framework</td>
</tr>
<tr>
<td>Trusted By</td>
<td>[ Array of entries ]</td>
<td>other GCCN Trust Registry Network entries attesting to trust in entity</td>
</tr>
<tr>
<td>Compliance Certifications</td>
<td>[ Array of entries ]</td>
<td>Jurisdiction or Industry compliance certification URI, URL</td>
</tr>
<tr>
<td>Classifications</td>
<td>[ Array of entries ]</td>
<td>Name value pairs of classifications and classification value. E.g. NAICS:01234</td>
</tr>
<tr>
<td>Meta tags</td>
<td>[ Array of entries ]</td>
<td>Meta tags defined by each entry</td>
</tr>
<tr>
<td>Text Description</td>
<td>string</td>
<td>Entity description</td>
</tr>
</tbody>
</table>

57
GCCN Trust Registry Network - Starting Definition

Summary Points

a. The lack of existing full featured Trust Registries open for discovery and queryable ‘evaluation’ makes the task of bootstrapping a network of such entries more difficult

b. GCCN will have to pursue engaging the ‘trust network’ candidates to determine how/ if it’s possible to interact with each in order to access information relevant for network entry updates
   i. Discovery is required to determine if ‘trust network’ parties are willing to provide this information

c. Access to a form based representation of entries sufficient to start
   i. Human readable as a web based form
   ii. Machine readable as json document
Open Conversation
Legal Notices

The Linux Foundation, The Linux Foundation logos, and other marks that may be used herein are owned by The Linux Foundation or its affiliated entities, and are subject to The Linux Foundation's Trademark Usage Policy at https://www.linuxfoundation.org/trademark-usage, as may be modified from time to time.

Linux is a registered trademark of Linus Torvalds. Please see the Linux Mark Institute's trademark usage page at https://lmi.linuxfoundation.org for details regarding use of this trademark.

Some marks that may be used herein are owned by projects operating as separately incorporated entities managed by The Linux Foundation, and have their own trademarks, policies and usage guidelines.

TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates.

Facebook and the “f” logo are trademarks of Facebook or its affiliates.

LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks or trademarks of LinkedIn Corporation and its affiliates in the United States and/or other countries.

YouTube and the YouTube icon are trademarks of YouTube or its affiliates.

All other trademarks are the property of their respective owners. Use of such marks herein does not represent affiliation with or authorization, sponsorship or approval by such owners unless otherwise expressly specified.

The Linux Foundation is subject to other policies, including without limitation its Privacy Policy at https://www.linuxfoundation.org/privacy and its Antitrust Policy at https://www.linuxfoundation.org/antitrust-policy, each as may be modified from time to time. More information about The Linux Foundation's policies is available at https://www.linuxfoundation.org.

Please email legal@linuxfoundation.org with any questions about The Linux Foundation’s policies or the notices set forth on this slide.