Advance Readings

In advance of the design workshop, all participants produced a one-or-two page advance reading to be shared with the other attendees on either:

- A specific problem that they wanted to solve with a web-of-trust solution, and why current solutions (PGP or CA-based PKI) can't address the problem?
- A specific solution related to the web-of-trust that you'd like others to use or contribute to?

If you will be attending Rebooting the Web of Trust Fall 2022 in The Hague, Netherlands, please upload your advance readings to this directory with a pull request.

Pull Request Submission

To add a paper, create a pull request to this repo with your contribution (preferably as an .md file, but if you can't, as a PDF), along with updates to the README.md in this folder. Please also include a byline with contact information in the paper itself.

Please also enter your paper *twice* in this README file, once in the topical listing (adding a new category describing your topic, if necessary) and one in the alphabetical listing. Please be sure to include the full URL for your paper in the README, so that we can copy it to the main page URL and have it still correctly link.

If you don't know how to submit a pull request, please instead submit an issue.

Request RWOT11 discount code

To those who have submitted an Advance Readings paper, RWOT11 offers a steep discount on the ticket price for participation to the event. Please obtain your discount code as follows. * Copy the link to your Pull Request (see previous section) * Email to questions@weboftrust.info, paste the link to the Pull Request and ask for the discount code

Please make sure to make your Pull Request Submission BEFORE you buy the tickets for RWOT11, in order to apply your discount code.

Primer Listing

These primers overview major topics which are likely to be discussed at the design workshop. If you read nothing else, read these. (But really, read as much as you can!)

- Advance Reading Primer — About the advance reading papers
- RWOT Primer — How the design workshop works

- DID Primer — Decentralized Identifiers (extended version also available)
- Functional Identity Primer — A different way to look at identity
- Verifiable Credentials Primer — the project formerly known as Verifiable Claims
- Glossary of Terms — a brief dictionary of technical terms used at RWOT
- Data Generator — a data-generator for SSI

Topical Listing

Please add a level three header (`###`) for your paper's topic if it's not there already, then link it in the form:

```
[name](link)
   * by [author](mailto:if desired)
   * One to two sentence synopsis or quote
   * #hashtags for topics
```

A Human Rights Approach to Digital Identity Protocols

- by Adrian Gropper, MD, Patient Privacy Rights, Austin, Texas
- A novel approach to digital identity protocols is presented that gives market power to the human subject of identity-based interactions through their ability to choose a delegate.
- #Delegation #HumanRights #DID #VerifiableCredentials #w3c #GNAP

A Minimal Approach to Linked Trust with Uncertainty

- by Golda Velez, Cooperation.org, Tucson, Arizona
- A pragmatic approach to enabling any observer to add to the linked trust ecosystem through observed claims. In particular applications to human rights and accountability, and the importance of broad adoption in heterogeneous domains in order to resist bad actors and provide aggregate privacy.
- #Adoption #HumanRights #AI #risk #trust #hybrid #VerifiableCredentials

Accessible self sovereign identity

- by Andrew Slack, SICPA, Switzerland
- and Victor Martinez, SICPA, Switzerland
- The experience and security of any system operated by people depends on the information conveyed through user interfaces, the response of the users, and the interpretation of their actions. Existing interaction patterns in verifiable credential wallets tend towards visual-centric models and rely on inconsistent representations of data. This paper explores design patterns to manage and exchange verifiable data in more accessible ways.
- #Accesability #VerifiableCredentials

Advanced DIDComm Messaging - A modern DIDComm based chat protocol

- by Karim Stekelenburg, Animo Solutions, The Netherlands
- Leveraging DIDComm to create a modern chat protocol that can compete with commonly used chat applications like WhatsApp and Telegram.
- #DIDComm #protocol #messaging #chat

AI & Metaverse - How to trust our digital twin?

- by Zaïda Rivai, Danube Tech Gmbh, Vienna
- A proposal of critical ethical issues in the emerging technology AI & metaverse. What are the most important (ethical) issues regarding trust, AI and metaverse? How could we solve them? How could we fight bias fed in AI algorithms used for the metaverse or how to solve the intellectual property problem in the metaverse?
- #ai #metaverse #trust #ethics

Analysis of hybrid wallet solutions - Implementation options for combining x509 certificates with DIDs and VCs

- by Carsten Stöcker, Spherity GmbH
- and Christiane Wirrig, Spherity GmbH
- The EU Commission's proposal for review of the eIDAS Regulation from 2021 has opened strong expectations for a deep change in traditional identity models. The EU might endorse a hybrid solution consisting of x509 certificates and decentralized PKI using DID/VC. This paper provides various options to address different implementation alternatives in combining x509 and DID/VC approaches.
- #did, #eIDAS, #x509, #hybrid-wallets

AnonCreds: ~~Ledger~~ VDR Agnostic Authentic Data Specification and Roadmap

- by Stephen Curran, Cloud Compass Computing Inc., Canada
- Adding details to the roadmap of the AnonCreds Specification Working Group about the use of AnonCreds with even more ledgers/VDRs, and the next version of the AnonCreds specification (and open source implementations), likely to be based on BBS+ Signatures.
- #DIDComm, #credentials, #privacy, #zkp, #DIDs, #DIDMethods

Audited DIDComm connections

- by Fabrice Rochette, 2060.io
- A discussion of how to make audited and intermediated DIDComm connections
- #DIDComm #protocol #messaging #chat

Authorized Issuer Lists

- by Manu Sporny, Digital Bazaar, USA
- A way of publishing a list of authorized issuers to enable Verifiers to bootstrap into trusted ecosystems.
- #VerifiableCredentials #w3c #trust #registries

BTCR From First Principles

- by Kate Sills, Digital Contract Design
- This paper compares did:btcr v0.1 to a naive, off-chain version in terms of vulnerabilities to a few identified attacks.
- #did:btcr #did #registry

Caching in DID Resolution

- by Markus Sabadello, Danube Tech, Austria
- Some thoughts on how to add and control caching in DID Resolution processes.
- #did #did-resolution

CESR adapter for sophisticated multisig

- by Henk van Cann, Blockchainbird.org, The Netherlands
- Bridge Keep wallet of KERI / ACDC and the more sophisticated solutions at BCC for keeping secrets secret. At the same time: study and work towards KERI, CESR and ACDC supporting sophisticated multisignature schemes.
- #SeedTool #KERI #CESR #ACDC #KEEP #ToIP #BCC

Collaborative Seed Recovery: A New Methodology for Smart Custody

- by Christopher Allen, Shannon Appelcline & Wolf McNally, Blockchain Commons
- Personally held digital assets are very vulnerable to accidental loss. This reading outlines solutions to date and looks at plans for a collaborative seed recovery architecture.
- #recovery #seed

Combining eIDAS High device binding with unlinkability

- by Sietse Ringers
- Strong device binding using ECDSA in order to achieve eIDAS High may be combined with unlinkability in SSI systems at the cost of introducing a TTP which deals with the linkability introduced by ECDSA.
- #ssi #eidas #credentials #privacy #zkp

Comparing Credential Formats

- by Dr. Andre Kudra, esatus AG, Germany
- Credential Formats analyzed and compared by an international expert group
- #Credentials #Formats #Signature #Revocation #Key-Management

Continuous Authentication and Authorization using Verifiable Credentials

- by Nikos Fotiou, Athens University of Economics and Business
- Verifiable Credentials for expressing user capabilities, issued using OAuth 2.0, and used for accessing HTTP-based resources that abide by the Zero-Trust principle.
- #IAA, #VerifiableCredentials, #ZTA

Creative Brief RWOT Animation Project.

- by Erica Connell, Legendary Requirements
- Let's produce a ~1-minute animation that tells the story of DIDs and RWOT. Working with collaborators from RWOT11, we will develop creative ideas and set the framework for the realization of a brief, stop-motion animated short.
- #RWOTAnimation #DIDs #changetheworld #attendRWOT

Credentialing-enabled Zero Trust Architecture for supply chains

- by Carsten Stöcker, Spherity GmbH
- and Christiane Wirrig, Spherity GmbH
- ZTA is an important design philosophy to establish security mechanisms at the API layer of each individual IT resource for increasing API Endpoint Security. This paper discusses how credentials can enable ZTA mechanisms to secure ERP systems for supply chain use cases.
- #ABAC, #API-Endpoint-Security, #Authorisation, #Credentials, #SupplyChain, #Wallets, #ZTA

Data exchange agreements - Making data transactions trustworthy, auditable and immutable

- by Lal Chandran, iGrant.io, Sweden
- A novel approach to building lawful, human-centric and scalable data spaces, making data transactions trustworthy, auditable and immutable via data exchange agreements. It provides a suite of tools that enable automated agreement handling for data exchange between a Data Source (DS) and Data Using Service (DUS). It helps organisations to be transparent and legitimate in their data usage while leveraging their data assets. Automated agreement handling is required for a scalable and regulatory-compliant

data marketplace (data space). It also provides individuals control over how their data is used and exchanged.
- #eSSIF-Lab #SSI-ecosystem #dataagreeents #rightdata #dataexchangeagreements #gdpr #privacybydesign

Decentralized revocation of Verifiable Credentials

- by Andrea Scorza, LTO Network, Arnold Daniels, LTO Network
- #Revocation #VerifiableCredentials #StatusList #Cryptography #bitstring #blockchain #LTO #Sovrin

Defining a BIP 322 Signature Suite

- by Will Abramson, Legendary Requirements, work funded by Digital Contract Design
- Let's make BIP 322 smart signatures a usable verification method for Verifiable Credential use cases.

DID Connect, connecting people, devices and applications via DID and Verifiable Credentials

- by Robert Mao, ArcBlock, United States
- DID Connect is a suite of RESTful APIs, UX components and SDK that provide a framework for DID interactions, connecting people, devices and applications via DID and Verifiable Credentials.
- #connect #application #framework #VerifiableCredentials #UX

DID Fluidity

- by Juan Caballero, Centre.io, Berlin/United States
- It would be great if a group of researchers and/or coordinators across DID methods could write lightweight micro-implementation guide covering cross-DID-method capabilities, anchored in properties defined in the DID data model and/or traits (see other paper below). This could be folded in as a section of the official W3C implementation guide at a later date if appropriate.
- #documentation #crosschain #crossmethod #portability #metawallet #DIDextensions

Did Resources for SSI - address ALL requirements via DIDs

- by Mirko Mollik
- DIDs allow us today to request the public keys to validate signature from a distributed verifiable data registry. Why not addressing all required resources like that, but independent from one specific vdr?
- #did #vdr #resources

DID Torrent

- by Vinay Vasanji
- A proposal to specify a p2p DID Method using the BitTorrent DHT, and a consumer use-case to drive its large scale adoption.
- #DIDs #DIDmethods #p2p #peertopeer #applications #wallet

DID Traits

- by Charles Cunningham and Wayne Chang, Spruce Systems, Inc., Berlin/New York
- A proposal for characterising and categorising DID methods by supported feature sets to evaluate technical suitability for different use cases, applications and environments.
- #dids #didmethods #identitymanagement #applications #devx

Discovery Handshake

- by Snorre Lothar von Gohren Edwin, Diwala, Uganda/Oslo
- A proposal to reason about bringing your own wallet to the table.
- #discover #protocols #wallet

DKMS for SSI

- by Philippe Page
- DKMS-4-SSI is driven by the need of security for a Dynamic Data Economy. By design DDE transactions take place in a Zero-Trust environement and relies on assymetric cryptography (public/private keys) to create/use/verify self-addressing idenitfiers (SAID).
- #eSSIF-Lab #SSI-ecosystem #key-management #keri #cesr

Dynamic & Decentralized Reputation for the Web of Trust: What We Can Learn from the World of Sports, Tinder, and Netflix

- by Ankur Banerjee
- A discussion on the potential drawbacks of proof-of-authority and soulbound tokens (SBTs), with an alternative system that could be constructed using Elo rating systems used in the world of sports and web services.
- #reputation #trust #scoring

Elision, Redaction, and Noncorrelation in Smart Documents

- by Wolf McNally, Christopher Allen, Shannon Appelcline, Blockchain Commons
- An introduction to the `Envelope` data structure and its novel approach to facilitating the construction and transformation of "smart documents", including native facilities for encryption, signing, elision (redaction), sharding, and noncorrelation.

- #VerifiableCredentials #identity #sharding #signing

Enabling SSI for NFC, IoT and other smart devices

- By Caspar Roelofs and Carlos Fontana, Gimly, the Netherlands
- An exploration of technical requirements, limitations and solutions to implement SSI with low-computational smart devices and low bandwith data-transmission such as NFC smartcards, IoT devices, NFC, BLE communication.
- #NFC #IoT #BLE #DIDComm #Inclusion

Enhancing DIDComm messaging for mobile environments

- by Ariel Gentile
- An exploration on different needs to make DIDComm-based mobile wallets interoperable and aware of the constraints given by mobile environments
- #DIDComm #protocol #messaging #Mobile #communications

eSSIF-Lab: Towards a European SSI ecosystem

- by Oskar van Deventer, TNO, Netherlands
- Overview of the eSSIF-Lab SSI ecosystem. "eSSIF-Lab is a 7 M€, three-year (2019-2022), European-Commission-funded program that has been sponsoring start-ups, SMEs and innovators to develop open-source SSI components, SSI products and SSI services."
- #eSSIF-Lab #SSI-ecosystem #Europe

Generalizing Secure Scuttlebutt for Data Integrity

- by Charles E. Lehner, Spruce Systems, Inc., New York
- A proposal for generalizing the Secure Scuttlebutt system for DIDs and Data Integrity.
- #VerifiableCredentials #SecureScuttlebutt

Identified communications - SSI and internet communications or internet communications and SSI

- by Alex Blom, Bloqzone, Netherlands
- Examining different solutions to the problem of identified communications
- #SIP #DIDComm #chat #communications

Identity and Trust in a Co-operative Ecosystem

- by Nick Meyne from Co-op Credentials
- Systemic approaches to the design of a digital identity and trust network for a co-operative ecosystem
- #identity, #trust, #community, #platform_co-operatives, #ecosystems, #systemic_design

Identity Bridge: Verifiable Credentials from European Digital IDs

- by Fabio Tagliaferro, Commercio.Network & University of Verona, Italy
- Leverage the power of national European identities to obtain SSI credentials, starting from the Italian SPID ecosystem.
- #VerifiableCredentials #Europe #SPID #Italy #SSI

Identity Net: Building an identity net through self-authenticated data graphs

- by Christopher Chung
- An emergent identity mesh built from authenticated data points
- #webs-of-trust #data #authentication #community #network

Multi-dimensional reputation systems using Webs of Trust

- by Oliver Klingefjord, Replabs, Berlin.
- A proposal for a novel multi-dimensional reputation system framework for social media using language models and webs of trust.
- #Reputation #Webs-of-trust #Trust-networks

On-Chain DIDs

- by Martin Riedel, Identity.com
- Evaluating DID (Document) State on-chain and the challenges around nomenclatures and spec-compliance.
- #dids #didmethods #identitymanagement #applications

Reducing Correlation: To What Degree is it Necessary?

- by Brent Zundel, Avast s.r.o.
- A proposal for a conversation about whether reducing correlation is necessary during credential exchange.
- #VerifiableCredentials #HolderBinding #Zero-knowledge-proofs #ZKP

Rendering Verifiable Credentials

- by Manu Sporny, Digital Bazaar, USA
- A Verifiable Credential extension to support rendering using graphics, audio, or braille.
- #VerifiableCredentials #w3c #a11y

Revisiting Usefulness of Centralized System for Establishing Trust

- by Shigeya Suzuki, Ph.D, Project Professor, Graduate School of Media and Governance, Keio University, Japan
- Using DNS as root of trust with help of ICANN's virtualized decentralized governance mechanism

- #RootOfTrust #DNS #DNSSEC #ICANN #VirtualizedDecentralization #MultistakeholderGovernance ### Revocation and VC
- by Ahamed Azeem, Danube Tech, Austria.
- A discussion about revocation methods used in SSI and VC and describes a suitable approach for privacy-preserving revocation.
- #Revocation #VC #RevocationLists2020 #IndyRevocationn

Self Custody Risk Analysis

- by Eric Schuh, Legendary Requirements, USA
- A software framework to enable the choice of how to self custody digital assets
- #recovery #wallet #threat-model

Social Wallet Recovery

- by Timo Glastra, Animo Solutions, The Netherlands
- Social recovery of wallet data and keys by leveraging sharding.
- #recovery #wallet #sharding

Societal impacts of SSI technologies

- by Amy Guy
- How can we make it easier to ask the hard questions about the work we do?
- #ethics #SSI-ecosystem #community

Spendability of Currency: Citizen Report

- by Will Abramson, Legendary Requirements, UK
- How easy is it to spend cash around the world these days? Let's find out, by actively attempting to and recording the results.

SSI data Generator

- by Moritz Schlichting, Animo Solutions, Utrecht, The Netherlands
- A data generator for SSI interactions and mocking
- #eSSIF-Lab #SSI-ecosystem #Europe #Data #Generator #tools

Standardization Overview

- by Maaike van Leuken, TNO, Eindhoven, The Netherlands
- An overview of SSI standardization
- #eSSIF-Lab #Standardization

Trust Registries – Enhancing Interoperability and preventing Phishing/MITM Attacks

- by Isaac Henderson Johnson Jeyakumar, University of Stuttgart, Germany & Michael Kubach, Fraunhofer IAO, Germany.
- A proposal for a Trust Registry concept to enhance interoperability and prevent Phishing/MITM attacks in different components of the SSI Ecosystem.
- #TrustRegistry #TRAIN #trustworthiness #SSI #eSSIF-Lab

Trusted Crypto Asset Framework

- by: Belsy Yuen, Elena Chachkarova, Egidio Casati
- A proposal for a decentralised trust framework powering regulated crypto assets
- #crypto-asset #ssi #regulated-deFi #kYC #smart-contract-wallet #on-chain-verifier

Unravelling Web of Trust

- by Ian Grigg
- By way of anecdotes, an exploration as to why WoT didn't work, and why Trust is harder. A request for more anecdotes to shed light on the way forward.
- #WOT #web-of-trust #trust #community

Using MultiBase Anchors within a Personally-Issued Endorsement Credential to Corroborate Attributes in an Existing Issued Credential

- by Phillip D. Long, Dmitri Zagidulin, Kerri Lemoie
- A proposal for a Verifiable Endorsements mechanism for VCs.

Validation - The Missing Link

- by Rieks Joosten, TNO, Netherlands
- In order to adopt VCs (or SSI technology), we need to explore what individual parties need *apart* from what's already part of VCs (e.g.: proofs), and how such needs can (also) be accommodated.
- #validation #verification #sovereignty

Verifiable Credentials Holder Binding

- by Oliver Terbu, Spruce Systems, Inc., Berlin/New York
- A proposal how to define a flexible and deterministic approach to verify the binding between the holder and the credential subject of the verifiable credential which is a blindspot of the W3C Verifiable Credentials Data Model 1.0 standard today.
- #VerifiableCredentials #HolderBinding #2FA #Biometrics #Delegation

Verifiable Identifiers

- by Joe Andrieu, Legendary Requirements, Ventura, CA, USA
- *A Best Practice for Decentralized Identifiers* Verifiable Identifiers (VIDs) are a DID best practice for platform-independent, privacy-agile, cryptographic verification of actions taken on behalf of that identifier.
- #DID #VID #IID #best-practice

Verifier Universal Interface

- by Daniel Moledo
- VUI (Verifier Universal Interface) specification proposal to achieve interoperability for the verification process: that is, to eliminate a possible vendor lock-in between any wallet and any verifier tool.
- #VerifiableCredentials #Verifier

Words Matter: A Rethink of Current SSI Terminology

- by Ana Goessens
- Continuing the conversation on the topics surrounding SSI, using methods from commercial branding to semantic philosophy.
- #Terminology #Semantics

ZKPs with zkSNARKs in a DIDComm ecosystem

- by Berend Sliedrecht, Animo, The Netherlands
- A proposal on working with zkSNARKs within the verifiable credential space
- #VerifiableCredentials #ZKP #zksnark

. . . more . . .

Alphabetical Listing

Please also enter your paper alphabetically in the form:

```
* [Paper Name](link)
```

- A Human Rights Approach to Digital Identity Protocols
- A Minimal Approach to Linked Trust with Uncertainty
- Accessible self sovereign identity
- Advanced DIDComm Messaging - A modern DIDComm based chat protocol
- AI & Metaverse - How to trust our digital twin?
- Analysis of hybrid wallet solutions - Implementation options for combining x509 certificates with DIDs and VCs
- AnonCreds: ~~Ledger~~ VDR Agnostic Authentic Data Specification and Roadmap
- Audited DIDComm
- Authorized Issuer Lists

- BTCR From First Principles
- Caching in DID Resolution
- CESR adapter for sophisticated multisig
- Collaborative Seed Recovery: A New Methodology for Smart Custody
- Combining eIDAS High device binding with unlinkability
- Comparing Credential Formats
- Continuous Authentication and Authorization using Verifiable Credentials
- Creative Brief RWOT Animation Project
- Credentialing-enabled Zero Trust Architecture for supply chains
- Data exchange agreements - Making data transactions trustworthy, auditable and immutable
- Decentralized revocation of Verifiable Credentials
- Defining a BIP 322 Signature Suite
- DID Connect, connecting people, devices and applications via DID and Verifiable Credentials
- DID Fluidity
- Did Resources for SSI - address ALL requirements via DIDs
- DID Torrent
- DID Traits
- Discovery Handshake
- DKMS for SSI
- Dynamic & Decentralized Reputation for the Web of Trust: What We Can Learn from the World of Sports, Tinder, and Netflix
- Elision, Redaction, and Noncorrelation in Smart Documents
- Enabling SSI for NFC, IoT and other smart devices
- Enhancing DIDComm messaging for mobile environments
- eSSIF-Lab: Towards a European SSI ecosystem
- Generalizing Secure Scuttlebutt for Data Integrity
- Identified communications - SSI and internet communications or internet communications and SSI
- Identity and Trust in a Co-operative Ecosystem
- Identity Bridge: Verifiable Credentials from European Digital IDs
- Identity Net: Building an identity net through self-authenticated data graphs
- Multi-dimensional reputation systems using Webs of Trust
- On-Chain DIDs
- Reducing Correlation: To What Degree is it Necessary?
- Rendering Verifiable Credentials
- Revisiting Usefulness of Centralized System for Establishing Trust
- Revocation and VC
- Self Custody Risk Analysis
- Social Wallet Recovery
- Societal impacts of SSI technologies
- Spendability of Currency
- SSI data generator
- Standardization Overview

- Trust Registries – Enhancing Interoperability and preventing Phishing/MITM Attacks
- Trusted Crypto Asset Framework
- Unravelling Web of Trust
- Using MultiBase Anchors within a Personally-Issued Endorsement Credential to Corroborate Attributes in an Existing Issued Credential
- Validation - The Missing Link
- Verifiable Credentials Holder Binding
- Verifier Universal Interface
- Words Matter: A Rethink of Current SSI Terminology
- ZKPs with zkSNARKs in a DIDComm ecosystem
- ... more ...

RWOT10 Papers

You may also want to consult the papers from RWOT10, as that design workshop was cancelled due to COVID.