Member of
Online Privacy Network
Privacy Assurance Lab

Open Consent

Scoping Identity Trust

Scoping Privacy and Surveillance Risks: For SSI

Global
Global Privacy Rights
Rights

Mark Lizar - Nov 1, 2021

Smart Species

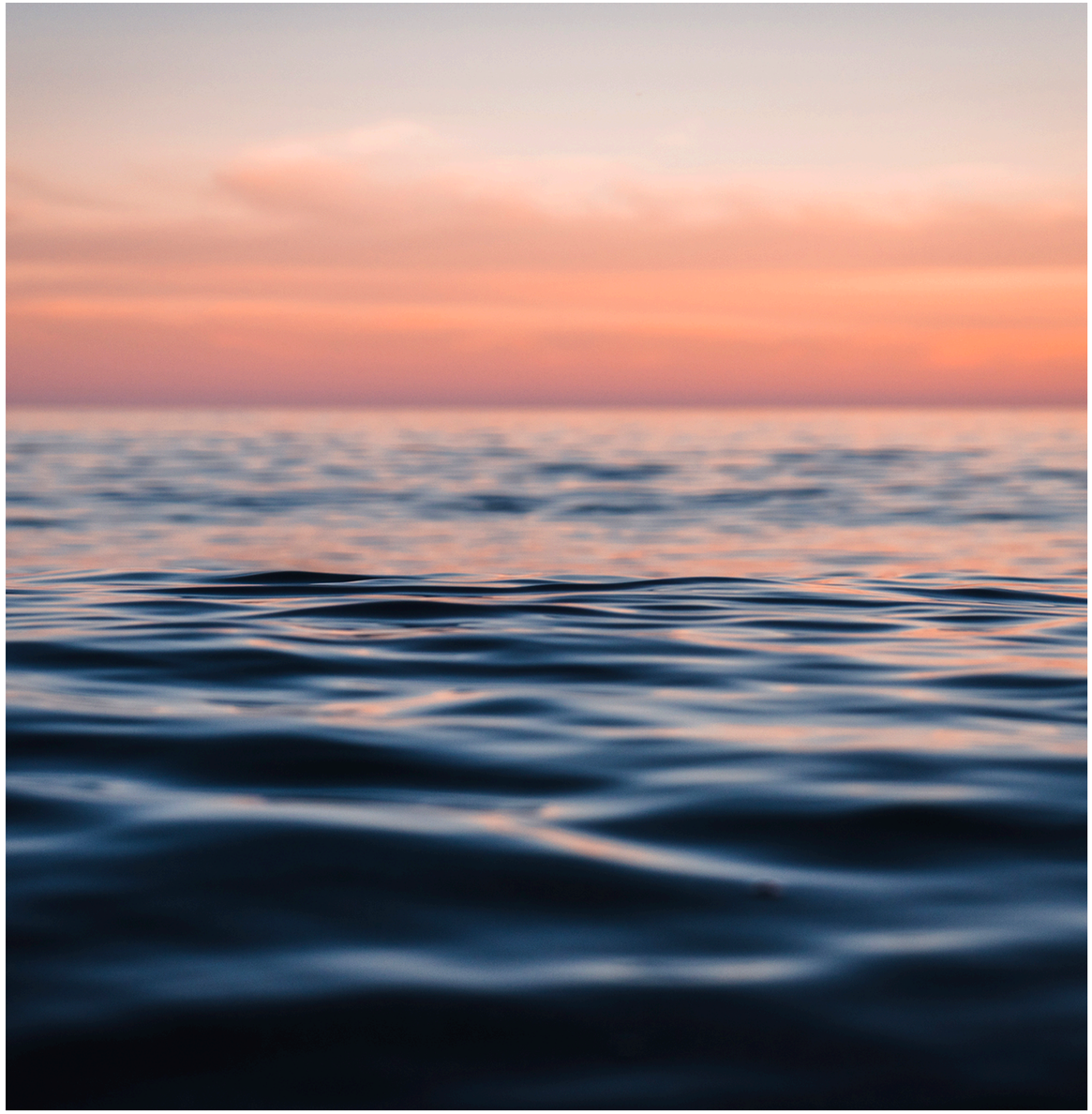
Online Privacy Notice

Active State Privacy

Privacy Assurance Laboratory

Try Privacy & Identity Risk Broadcasting

Twinning Privacy Notices
For Machine Readable Human Governance



2 Types of Identity Trust

Risk Assessing Both Type of Trust

1. Digital Identity Scope of Trust - Little ‘g’ Governance

- Scope of Risk for SSI (VC’s + ZKP + TPM)

2. Human Context Scope of Trust - Big ‘G’ Governance

- Scope of Risk for all surveillance of ones whole identity in a specific context separately for all instances of identifier

Scope of Risk (Digital Trust) SSI

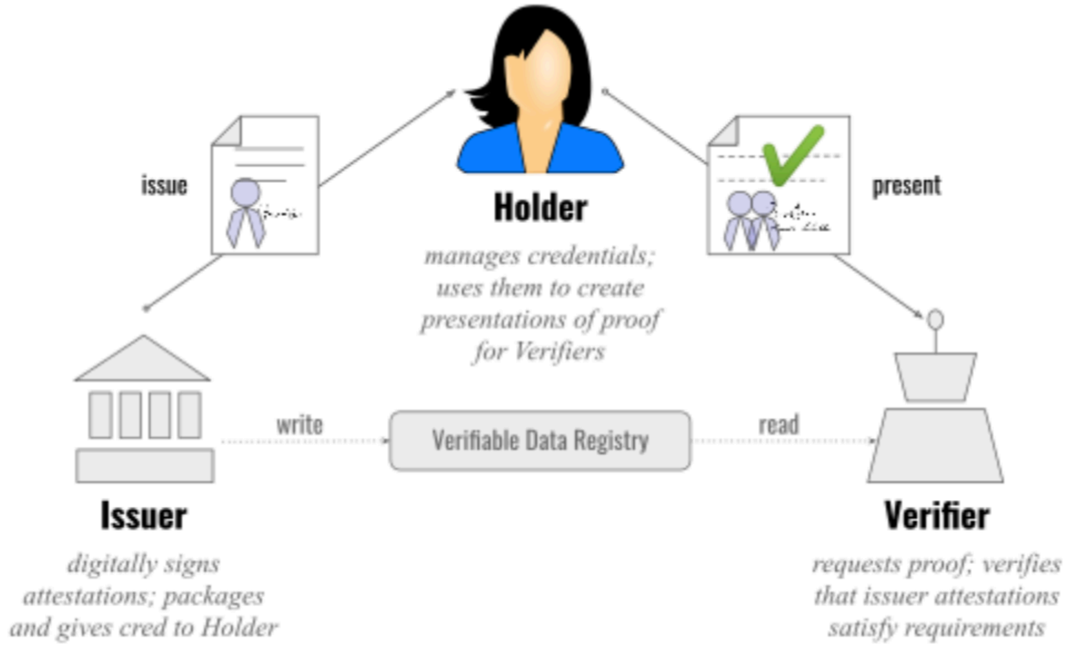
Focus of Privacy & Risk Task Force

Verifiable credentials

From Wikipedia, the free encyclopedia

This article **needs additional citations for verification**. Pleas
Unsourced material may be challenged and removed.
Find sources: "Verifiable credentials" – news · newspapers · books · schol
template message)

Verifiable credentials (VCs) are an open standard for digital credentials. They can represent information found in physical credentials, such as a passport or license, as well as new things that have no physical equivalent, such as ownership of a bank account. They have numerous advantages over physical credentials, most notably that they're digitally signed, which makes them tamper-resistant and instantaneously verifiable.[1][2] Verifiable credentials can be issued by anyone, about anything, and can be presented to and verified by everyone. The entity that generates the credential is called the *Issuer*. The credential is then given to the *Holder* who stores it for later use. The Holder can then prove something about themselves by presenting their credentials to a *Verifier*.



Digital No-Need to Trust

Zero Knowledge Proof

Zero-knowledge proof

From Wikipedia, the free encyclopedia

(Redirected from Zero knowledge proof)

"ZKP" redirects here. For the airport in Russia, see Zyryanka Airport. For other uses, see Zero knowledge.

In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.[1]

Identity Risk & Lifecycle

Identity Assurance for a context, instance, and its own data gov lifecycle

Security

Public Facing Context

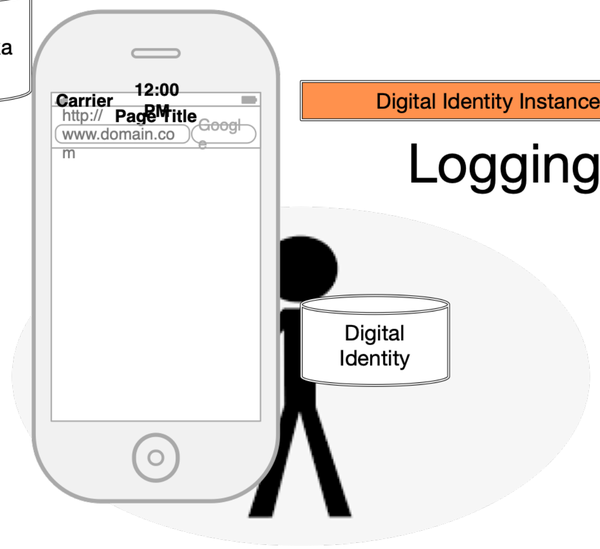
Social Perspective is identifying you!

Identity & Access Management

Device or Website

Physical Service aka phone

Digital Identity Instance

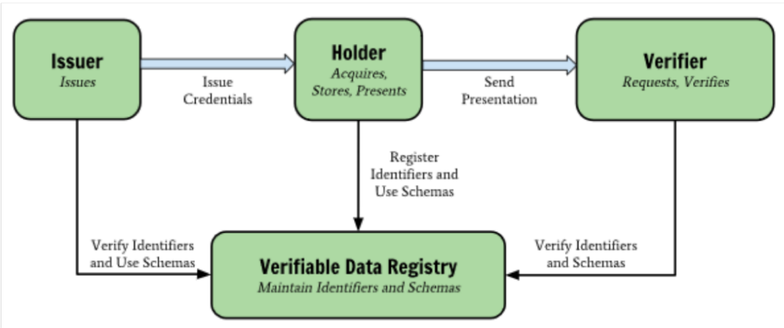


SSI Flow

Traditional

SSI

Logging in - User Name & Password



Data + Identity Tech Governance

Privacy & Surveillance Risk Assurance

Identity

From Wikipedia, the free encyclopedia

Identity may refer to:

Social sciences [edit]

- Identity (social science), personhood or group affiliation in psychology and sociology

The Privacy Cafe

Getting a Coffee at a Coffee Shop Requires Consensus

Coffee Shop

Social Agreement & Context

i. Social Agreement & Context

ii. Legal Agreement Context (s) Covering

iii. Technical Agreement Context

i. Wifi Access

ii. Mobile app (pre-ordering-Context)

iii. Video Surveillance

iv. Loyalty Card

v. Website

iv. Digital Identity Risk

i. In Contrast the SSI Risk

Human Control Risk Assurance

Including the human (pre-existing scope) & Digital Identity Risks

- Privacy Controller Credential Risk Assessment
- 3 Tiers of Active State Privacy Risk Assurance : Privacy & Identity Risk Assurance (3 scopes)

  1.Self-Asserted

  2.Legal & Accountabile Credential / Monitored

  3.Certified = Legal & Accountable + a monitored Code of Practice

WHiSSPR - Report

Operational Privacy Risks Reporting

- Categories of Risk: **W**hite **H**at **i**Dentity, **S**urveillance, **S**ecurity, **P**rivacy(by Default), **R**isk Reporting
  - WH Ethics = Context, Identity & Technology Agnostic - Operational Privacy / context specific assessment
  - Operational Privacy - How many iDentifiers/Session Instances per physical Context # of iDentity + tech - How many identifiers per context (not instance)
  - Assessed per Identifier that is shared & Disclosed in a context
    - e.g, a coffee shop
  - iDentity = who is the legal entity / who is the accountable / in controller and responsible
  - Surveillance = what identifier (and derivatives) are collected per context e.g biometric: video/ audio/ finger print
  - Security - how many different parties are identifiers/credentials disclosed to?
  - Privacy - for what purpose is digital identity system used for and what permissions does it provide

Digital Identity Privacy Risk (DiPR)

Surveillance Risk Assessment

Identity Control, Surveillance & Security DiPR

- what type of identifier
  - (or derivative) is a) created b) collected c) associated with the session / - e.g. video surveillance or verifiable credential, cookie, etc.
- Surveillance
  - Who controls the identifier /credential? (And in what context)
  - Is the PII Principal/Individual able to control the identifier? e.g. share identifiers on purpose? If so, Are additional identifier or assurances required to use the credential and identifier?
- Security
  - When disclosed is control transferred / shared and if so how many copies of the identifier are made ?
  - What other stakeholders will the identifier be disclosed /exposed to?
- Privacy Assurance
  - Is there a log of disclosures? Are the logs signed on each use?
  - Are any identifier disclosures notified ? And when/where/ how ? As apart of what purpose?
- What type of agreement and policy is used for governance disclosures?
  - How is the agreement enforced ?

Active State Privacy Tech

Decentralized Data Governance

OPN: Privacy Assurance Lab Sandbox

Sandbox's: Collaborative, 4p, Sponsored & Private - Privacy Tech Benchmarking & Active State Privacy Integration Privacy Broadcasting

- Universal UI/UX Privacy Risk Broadcasting
- Consent By Default
  - Consented Surveillance -
  - Alternate eConsent Authorization Flow
  - Privacy as Expected : Consent Gateway
- Tools, Assessment, Audits for Benchmarking and Improving Privacy & Identity Tech

{Privacy Broadcasting for Consent by Default UX }

OPEN CONSENT

OPN W.H.i.S.S.P.R-R's

White Hat: iDentity, Surveillance and Security, Privacy Risk Reporting

Privacy Assurance Lab

Get in touch to bench-Mark - Mitigate Risks with Global Identity Rights

BenchMark@Opn.org

Smart Species

People Intelligence