

TeleTrust/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 20.09.2022

SSI – A Highway to extinction of data leaks

Muhammad Rameez,

Deutsche Gesellschaft für Cybersicherheit mbh & Co. KG

Introduction



Muhammad Rameez

Team lead Blockchain Services,
DGC
Masters in Distributed Software
Systems from TU Darmstadt



We manage the risks of your digital transformation

As one of the leading providers of cyber security, DGC supports companies in taking advantage of the opportunities offered by the digital transformation – and in minimizing the associated risks.

Vision and philosophy

Make the internet secure

Services and Products

- ✓ cyberscan.io®
- ✓ Pentesting
- ✓ CDOC: Security Operation Center of tomorrow
- ✓ Blockchain

Location and Offices

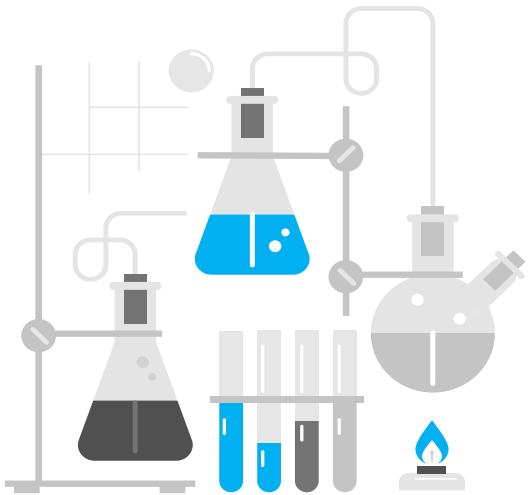
Berlin, Flensburg, Zurich, Abu Dhabi, Cologne



Warning: This presentation has



- Memes
- Pop culture references
- cliches



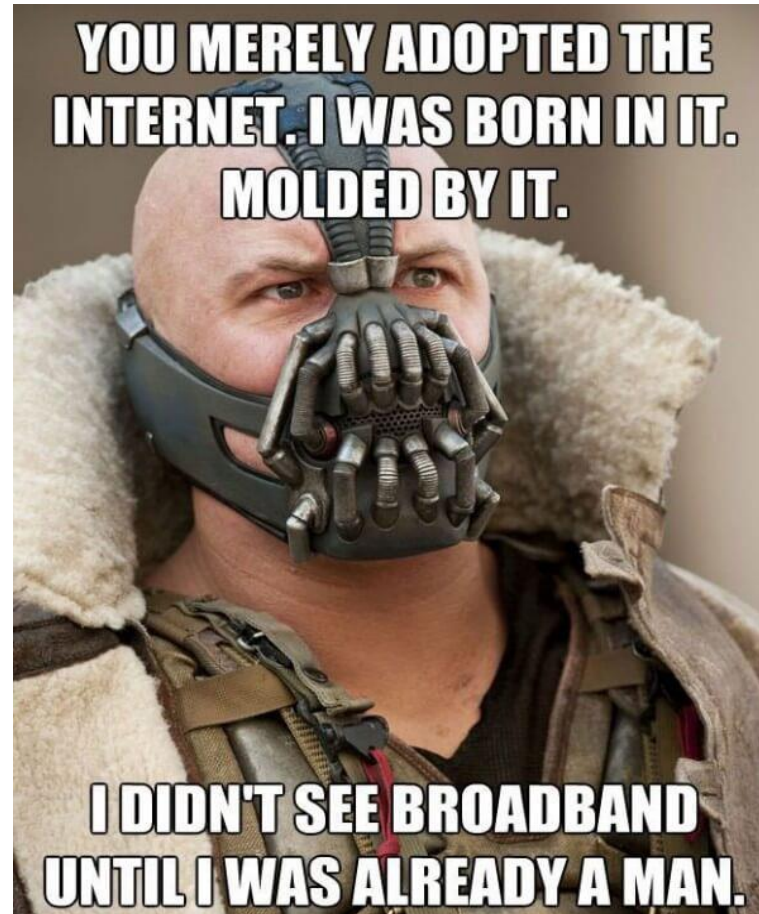
20.09.2022

Agenda



- Story of the internet
- Digitalization: Benefits and Challenges
- Solutions
 - SSI: as the cure
 - Benefits of SSI
 - Challenges

Dial up to broadband



The Ideals of the early internet



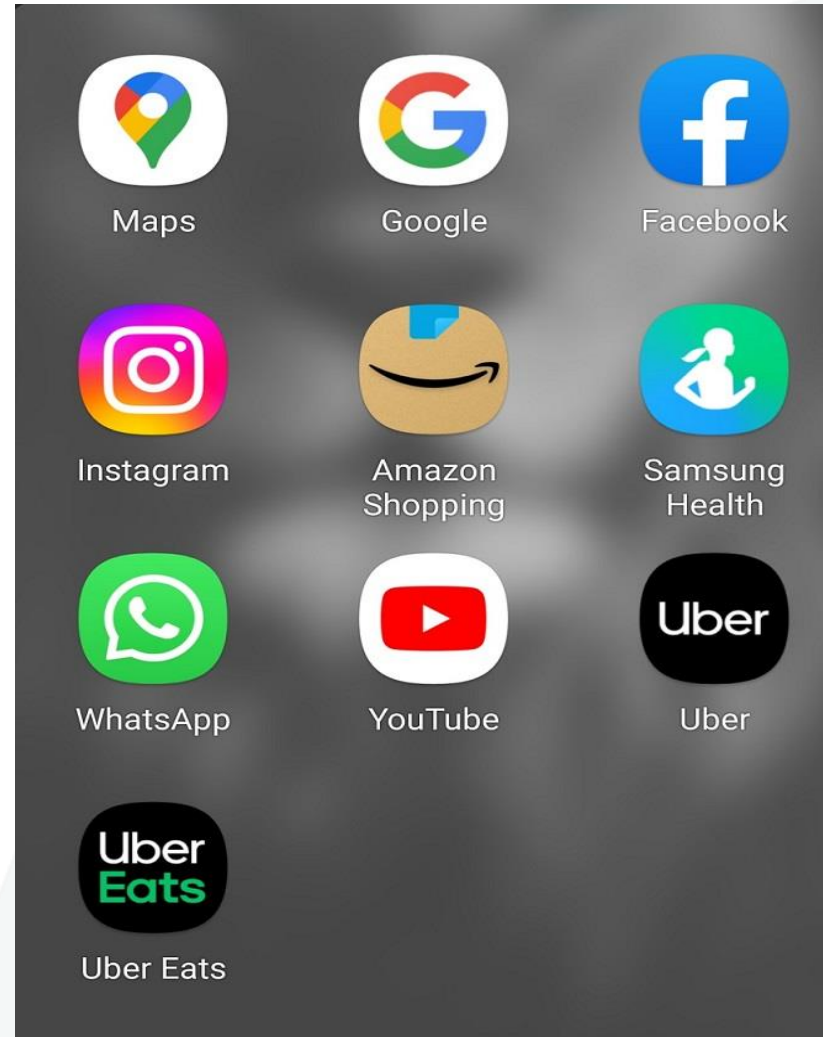
- Freedom of speech
- Free access to information
- Knowledge belongs to all mankind
- Collaboration and inclusion

Digital Revolution



- Always on
- Always connected
- On – Demand
- Just in time
- Next day delivery
- **Social media and the rise of influencer culture**

User relationship with tech giants



20.09.2022

The dawn of the Information age



Hack the World!



20.09.2022

11

The power of Social Media and big tech



- News reporting and journalism has been replaced with click bait articles.
- Revolutions are triggered through social media
- Perpetual Wars are being fought in the cyberspace – **war for our minds!**
- Elections and Referendums are being manipulated
- People reporting war crimes are being prosecuted

How did we get here?



- Desire to replicate real world processes in the cyber space.
 - Restricting access to products or functions
- Gate keeper functions and centralized data repositories
 - Access control
 - User data is persisted and replicated
- Digital fingerprints: A.P.I for influencing minds En Masse
 - Analyze
 - Predict
 - Influence

Digital fingerprints: The new Gold rush!



- New Gold rush for data!
 - Cybercriminals, Companies, Governments
- RIP privacy!
- Targeted misinformation campaigns



The top data breaches of 2021

- Android Users Data Leak — 100+ million. ...
- Thailand Visitors — 106+ million. ...
- Raychat — 150 million. ...
- Stripchat — 200 million. ...
- Socialarks — 214+ million. ...
- Brazilian Database — 223 million.
- Bykea — 400 million. ...
- 3. Facebook — 553 million.

[More items...](#) • 9 Dec 2021

[https://www.securitymagazine.com/articles/96667-the-...](https://www.securitymagazine.com/articles/96667-the-top-10-data-breaches-of-2021) :

The top data breaches of 2021 - Security Magazine



This is a screen shot from security magazine article: top data breaches of 2021

Online marketplaces selling user data



Dashboard

Genesis Wiki

News

Bots

Generate FP

Orders

Purchases

Payments

Tickets

Software

Profile

Invites

Logout

Home / Bots

new

15

320k+

Bots

BOT NAME/

Filter bot name

Any

RESOURCES KNOWN / OTHER

Filter resource name/domain: paypal,ebay.com,hotmail.com...

F5C20E55-9414907A-2DB46096-4C959543-8FE212AE

2019-12-01 20:08:52

2020-11-13 21:46:12

2 x

AppleStore

Steam

Facebook

com.contextlogic.wish

com.netflix.mediaclient

Google

Twitter

Zoom

com.manciukic.registro

...

Live

Amazon

...known 41

...other 108

D1854F8BF59E1F43848E3DBF193ACA17

2020-08-21 09:18:09

2020-11-13 21:45:51

2 x

Google

eu.battle.net

...

...known 1

...other 1

3796BE0F66FD2C4D66029B5F88BE0AE7

2020-10-31 23:38:34

2020-11-13 21:45:36

2 x

Google

Spotify

com.contextlogic.wish

accounts.epicgames.com

discord.com

Steam

bloxawards.com

api.20.leya.com

manuaiscolares.pt

...

Instagram

...known 8

...other 26

This Photo by f5 labs is licensed under CC BY-SA taken from online article genesis

20.09.2022

16

www.dgc.org

Deutsche Gesellschaft für Cybersicherheit. All rights reserved.©

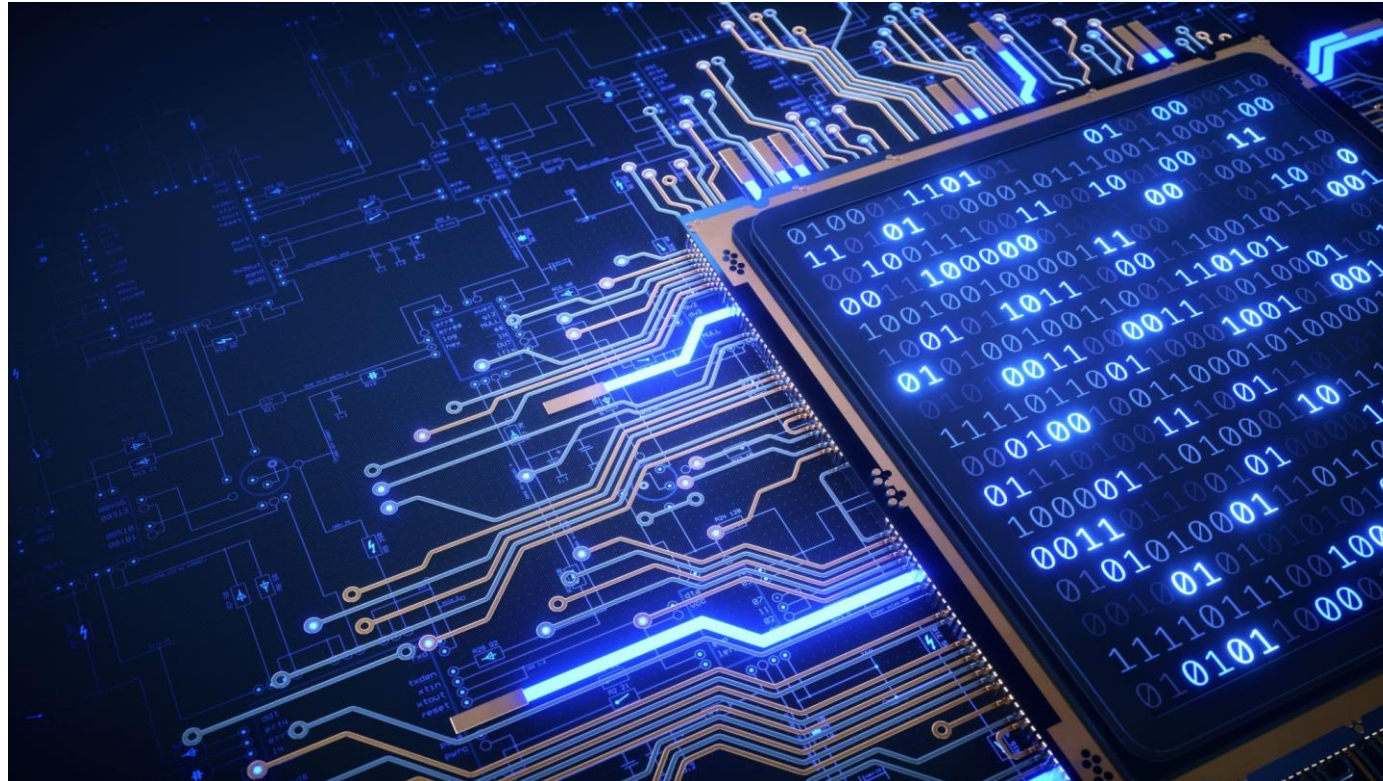
20.09.2022

16

What is the solution?



Increase the security of systems.



Reverse Digitalization



- Dial back the clock on digitalization
- Let's call in Doc Brown!
- **Look to our history to inform our future**



Self-sovereign identity: The secret third option.

SSI coupled with verifiable credentials could enable the next evolution of the internet

- ✓ Privacy preserving
- ✓ User data controlled by individuals
- ✓ Can eliminate data honeypots
- ✓ Data can be free from siloed systems
- ✓ Potentially making data leaks a relic of the past



Verifiable Credentials Data Model

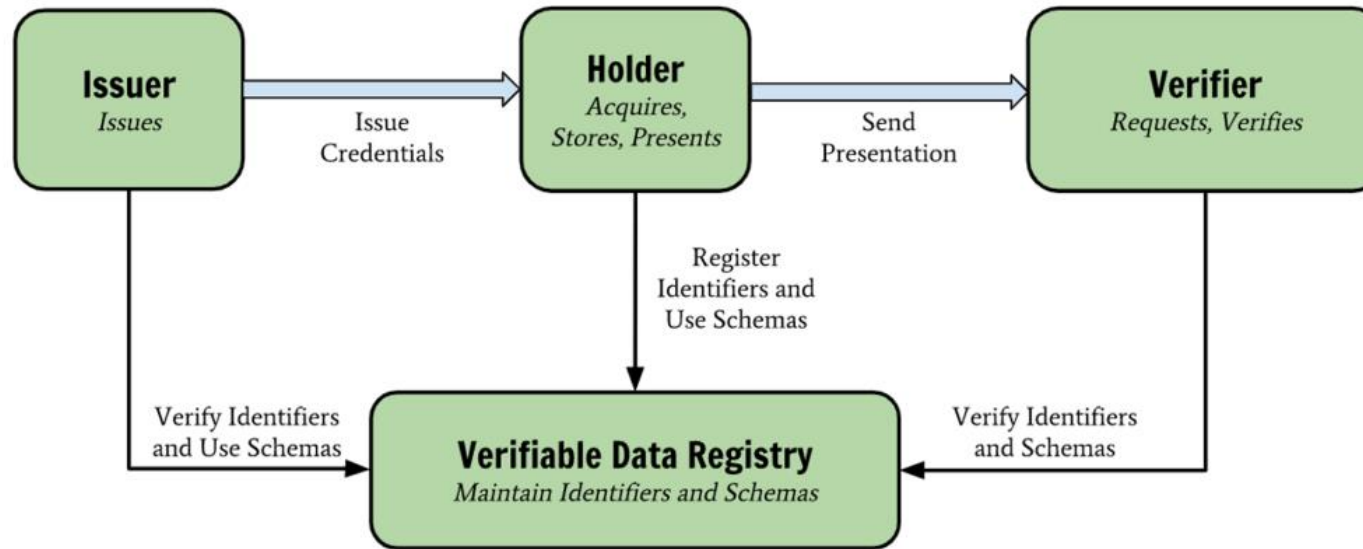


Figure 1 The roles and information flows forming the basis for this specification.

<https://www.w3.org/TR/vc-data-model/>

Challenges faced by the SSI Ecosystem



- Fragmentation and application-oriented approach
 - Decouple wallets from protocols / solutions
- Data is still being persisted
 - Credential issuer requires and persists some data to issue credentials
 - Verifiers can copy credentials and persist them due to regulatory requirements
 - Application itself saves credential data in local databases
- Need for Protocols and standards
 - IDunion
 - EEIDAS
 - W3C

Opportunities for the future!

SSI: Made in EU



- EU can take an important role in this.
 - Help shape the future of a secure and better internet
- Embrace new technologies
- BBS + ZKP verifiable credentials
 - No data is ever persisted.
- Create environment that fosters innovation
 - Cut the red tape
 - Talk to the stake holders -> policy makers and tech people
 - Don't be afraid of paradigm shifting realities -> adapt and embrace
 - Self custody
- Steps in the right direction
 - EEIDAS
 - ESSIF



- Focusing on an SSI solutions based on W3C recommendations
- The wallet can support many different DID standards and algorithms
- Two - dimensional Claim model
 - Claims are presented and verified but never stored
 - Anonymous arm band claims for access control
- Zero knowledge proofs



- <https://www.prospectmagazine.co.uk/magazine/morozov-web-no-utopia-twenty-years-short-history-internet>
- <https://startsmarter.co.uk/the-advantages-and-disadvantages-of-digitalisation/>
- <https://www.virtu.com/blog/8-benefits-digital-transformation>
- <https://www.cutimes.com/2019/08/28/the-rise-of-digital-fingerprints-in-the-dark-marketplace-threatens-identities/?slreturn=20220812130613>
- <https://damienbod.com/2021/10/11/challenges-to-self-sovereign-identity/>
- <https://damienbod.com/2021/05/31/verify-vaccination-data-using-zero-knowledge-proofs-with-asp-net-core-and-matrx/>
- <https://damienbod.com/2021/12/13/implement-compound-proof-bbs-verifiable-credentials-using-asp-net-core-and-matrx/>
- <https://www.securitymagazine.com/articles/g6667-the-top-data-breaches-of-2021>

Thankyou

