
ECCO
European Cybersecurity COmmunity
Empowering End Users through Self-Sovereign Identity: Privacy and Security by Design
European Cybersecurity Competence Centre (ECCC) ECCO
Community Group on Human Factors
19 November 2024

European Cybersecurity Competence Centre (ECCC) ECCO

Community Group on Human Factors

Kai Rannenberg / Narges Arastouei

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Objectives

- Build a community of experts and "end users" for the WG domain by initiating work on a sequence of prioritized topics in the WG domain
- Support selected actions prioritised in the ECCC Strategic Agenda matching the WG domain, especially within
  - 1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs
  - 1.2.3 Promote security and privacy 'by design'
  - 2.1.4 Promote security and privacy 'by design' approach in training and education

Methodology

- Start with actions related to one or several of the topics listed in the ECCO technical offer:
  - 5G applications, ICT in mobility, security of day-to-day tools like smartphones, web meeting systems and services, Internet access technologies, digital money.
- Deep dive on proposals for priorities for DEP or other appropriate support measures
- Build sub-groups as needed
- …

Matching: ECCC Strategic Agenda actions Topics from Technical Offer

Action/Topic	1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs	1.2.3 Promote security and privacy 'by design'	2.1.4 Promote security and privacy 'by design' approach in training and education
5G applications			
ICT in mobility			
Security of day-to-day tools, e.g.			
Smartphones			
Web meeting systems and services			
Internet access technologies			
Digital money			
…			
…			

Work on topics within the matrix prioritized by the community of experts and "end users"

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Identification of relevant achievements / best practices (e.g. developed in the ECCC pilots) to address the Strategic Agenda
  - 1st Webinar (March 8): **A Footprint of CyberSec4Europe: two prominent cybersecurity tools (Keynotes: Vashek Matyas et al, Masaryk University Brno, CZ)**
  - 2nd Webinar (May 22): **Security-by-design for SMEs exploiting trusted hardware (Keynote: Antonio Lioy, Politecnico di Torino, IT)**
  - 3rd Webinar (19 June): **Engaging Citizens and Civil Society in Cybersecurity (Dr. Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research)**
  - 4th Webinar (23 July): **LINDDUN GO, Lightweight & Gamified Privacy Threat Modeling (by Jonah Bellemans at the DistriNet Research Group of KU Leuven (Belgium)).**
  - 5th Webinar (16 September): **From Awareness to Action: Enhancing Parental Engagement in Online Privacy Protection (by Ann-Kristin Lieberknecht at Goethe University Frankfurt)**
  - 6th Webinar (23 October): **Security by Design through the Recursive InterNetwork Architecture [by Toktam Ramezanifarkhani, Associate Professor in Cyber security School of Economics, Innovation and Technology | Oslo, Kristiania University college & Peyman Teymoori, Associate Professor ,University of South-Eastern Norway (USN)]**

- Today's Webinar (19 November): **Empowering End Users through Self-Sovereign Identity: Privacy and Security by Design [by Dr. Mohsen Toorani, Associate Professor of Cybersecurity at the University of South-Eastern Norway (USN), Campus Kongsberg]**

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Recommendations for future specific priority "Joint Actions" (e.g. DEP projects) and other actions for the ECCC
  - Based on matching of goals with action types also considering the ECCC action plan
- Possible cooperation in immediate Joint Actions
  - Deep dive on specific topics: e.g. stemming from the needs of SMEs for easily accessible and user-friendly cybersecurity tools considering privacy
- Knowledge sharing events: presentations for EC, NCCs, ECCC
  - Webinars on the progress including refinement of the topics

ECCO
European Cybersecurity COmmunity

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

How to join the CG

- Email: community_humanfactors-owner@list.cyber-ecco.eu with your
  - Contact details
  - Affiliation and role therein
  - Area of expertise

Keynote & Speaker

- **Empowering End Users through Self-Sovereign Identity: Privacy and Security by Design**

In an increasingly digital world, enabling privacy-focused and user-controlled identity management is essential. Self-Sovereign Identity (SSI) is a decentralized approach that empowers individuals by giving them control over their digital identities without relying on centralized authorities. This webinar explores how SSI fosters privacy and security by design, promoting trust and supporting digital sovereignty across sectors such as healthcare, IoT, and beyond. Through real-world applications, we will examine SSI's potential to address critical security challenges, ultimately empowering end users and strengthening digital ecosystems.

- **Keynote Speaker: Dr. Mohsen Toorani**
  - Dr. Mohsen Toorani is an Associate Professor of Cybersecurity at the University of South-Eastern Norway (USN), Campus Kongsberg. He holds a Ph.D. in Information Security from the University of Bergen and has a background in Secure Communications (M.Sc.) and Communications Engineering (B.Sc.). He is a senior member of IEEE and a member of IACR. His research interests include cryptography, cybersecurity, and distributed systems security. He is actively involved in research projects, editorial roles, and conference organizations.

ECCO
European Cybersecurity COmmunity

ECCO Community-driven Knowledge Sharing Events

Disclaimer

- *These sessions are ECCOcommunity-driven and expert-led, reflecting the collective knowledge and contributions of the members of the ECCO Community Groups. They are designed as knowledge-sharing events to build/animate the cybersecurity Community Groups on key topics and share valuable insights among stakeholders.*
- *The information and opinions in this document are provided "as is" for general purposes only.*
- *Experts are encouraged to ensure their presentations are accurate and up-to-date.*
- *The views expressed in this webinar are purely those of the experts and may not, in any circumstances, be interpreted as stating an official position of the European Commission (EC), the European Cybersecurity Competence Centre (ECCC), the ECCO project, or any other EU institution, body or agency. The European Commission does not guarantee the accuracy of the information included in this webinar, nor does it accept any responsibility for any use thereof.*
- *References to specific commercial products, processes, or services do not imply endorsement or recommendation, and this webinar should not be used for advertising purposes.*


ECCO
European Cybersecurity COmmunity
Empowering End Users through Self-Sovereign Identity: Privacy and Security by Design
Mohsen Toorani
University of South-Eastern Norway
Kongsberg, Norway
November 19, 2024

Overview

- Introduction
- Challenges with Current Systems
- What is SSI?
- Core Components
- Regulatory Frameworks (GDPR, eIDAS2, NIS2)
- Sectoral Use Cases (Healthcare, IoT, Finance, Government Services)
- Security Challenges and Solutions
- Trends & Implementation Challenges
- Conclusion

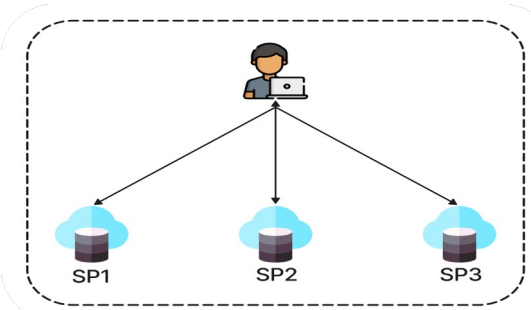
What is Self-Sovereign Identity (SSI)?

- SSI is a decentralized approach to digital identity, giving individuals full control over their data without relying on centralized authorities.

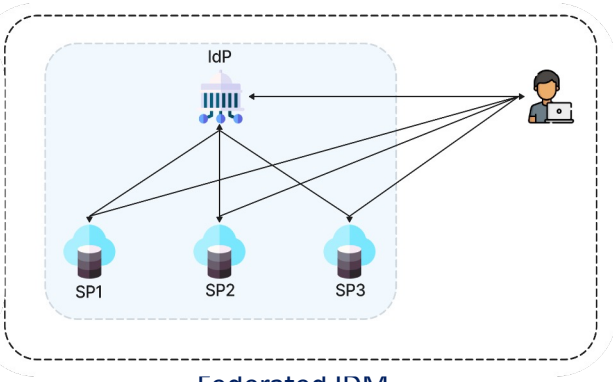
- **Core Features:**
  - **User Control:** Individuals create, own, and manage their identities.
  - **Privacy by Design:** Data minimization ensures only necessary information is shared.
  - **Trust Distribution:** Users determine who to trust with their information.

Traditional Identity Management Model

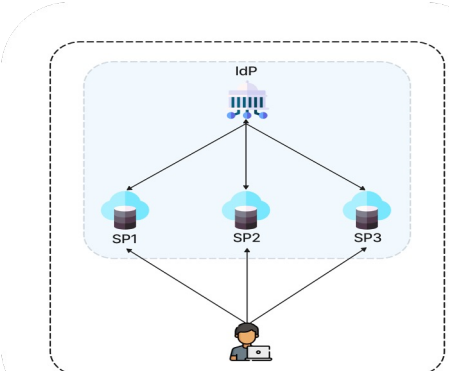
- **Centralized Systems:**
  - Relies on single authorities or intermediaries to manage identity.
  - **Examples:** Federated Identity (e.g., Google, Facebook) or isolated identity silos.
- **Limitations**:
  - **Privacy Issues**: Overcollection of user data without proper consent.
  - **Security Risks**: Single points of failure make these systems attractive to attackers.
  - **Lack of User Autonomy**: Users depend on central providers for identity access and recovery identities.



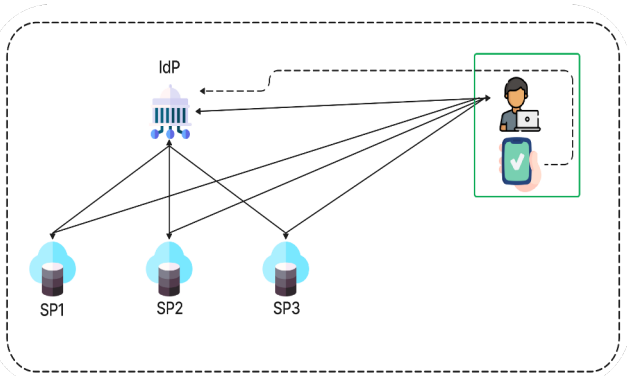
Isolated IDM



Federated IDM



Centralized IDM



User-centric IDM

Source: https://hdl.handle.net/11250/3131437

Challenges of Centralized Identity Systems

- **Data Breaches:** Centralized systems are attractive targets for hackers.
  - In 2023 alone, over 17 billion records were compromised globally due to breaches (Infosecurity Magazine).
  - The Equifax data breach affected 147 million Americans
  - Yahoo exposed data from 3 billion accounts in a single breach.
- **Privacy Concerns**:
  - Centralized systems often collect and store excessive personal data without proper consent.
  - Users lack visibility into how their data is used, increasing the risk of misuse.
- **Lack of User Control**:
  - Individuals rely on central authorities for identity verification and management which limits their direct involvement.
  - Limited transparency and autonomy result in reduced trust and control over personal data.
- **Interoperability Issues**:
  - Centralized systems operate in silos, making seamless interactions across platforms difficult.

Decentralized Identity vs SSI

- **Decentralized Identity:**
  - Removes reliance on central authorities by distributing identity management across systems.
  - Leverages **Decentralized Identifiers (DIDs)** and **Verifiable Credentials (VCs)** for secure interactions.
- **Self-Sovereign Identity (SSI):**
  - Key Differentiator:
    - SSI goes beyond decentralization, prioritizing **user autonomy, privacy, and trust**.
    - **Selective Disclosure**: Shares only necessary information for interactions.
    - **Privacy by Design**: Aligns with GDPR principles, reducing data exposure.

GDPR and SSI - Privacy by Design

- **User Control and Consent**:
  - SSI empowers users with full control over their data, supporting GDPR rights like access, rectification, and erasure.
  - Consent management tools allow users to share or revoke access easily.
- **Decentralization**:
  - SSI reduces reliance on centralized systems, minimizing risks of single points of failure.
- **Privacy-Enhancing Features:**
  - **Selective Disclosure:** Share only the necessary information, ensuring compliance with GDPR's data minimization principle.
  - **Advanced Cryptography:** Techniques like ZKPs ensure secure and private interactions.
- **Immutable Security:**
  - Blockchain and decentralized ledgers provide tamper-proof, transparent identity records, enhancing trust.

eIDAS2 and the European Digital Identity Wallet

- **eIDAS2:**
  - An updated EU regulation for secure, interoperable identity management across public and private sectors.
- **The European Digital Identity Wallet**
  - A unified platform for securely storing identity documents (e.g., passports, licenses).
  - Allows citizens to manage DIDs and VCs.
- **Key Features:**
  - **Cross-Border Interoperability:** Seamless access to public and private services across EU member states.
  - **User Control and Privacy:** Aligns with GDPR principles, enabling privacy-preserving and user-centric identity management.

SSI and Regulatory Frameworks: GDPR and eIDAS2

- **GDPR Alignment:**
  - SSI empowers users with tools for **consent management**, fulfilling GDPR requirements for data control.
  - **Selective Disclosure:** Ensures compliance with GDPR's principles of **data minimization** and **privacy by design**.

- **eIDAS2 Integration:**
  - SSI forms the foundation for the **European Digital Identity Wallet**, enabling cross-border identity management.
  - Facilitates **interoperability** and privacy-preserving digital interactions across EU member states.

SSI and NIS2

- **NIS2** reinforces cybersecurity for critical sectors like **healthcare**, **finance**, and **transportation**.

- **How SSI Aligns with NIS2:**
  - **Resilience:** Decentralized identity minimizes reliance on single points of failure.
  - **Authentication:** DIDs and VCs ensure robust identity verification for users and devices.
  - **Data Security:** Encryption protects data during storage and transfer, complying with secure exchange requirements.

eIDAS2 and NIS2: Milestones and Implementation

- **eIDAS2 Timeline:**
  - **November 2023:** Agreement on eIDAS2 standards, including the European Digital Identity Wallet.
  - **By 2026:** EU Member States to roll out wallets for cross-border services.

- **NIS2 Timeline:**
  - **January 2023:** NIS2 Directive entered into force.
  - **October 2024:** Member States must transpose NIS2 into national laws.
  - **Example:** Germany's **Cybersecurity Enhancement Act** (effective 2025) focuses on healthcare and finance, aligning with NIS2.

Standardization and Policy Support for SSI

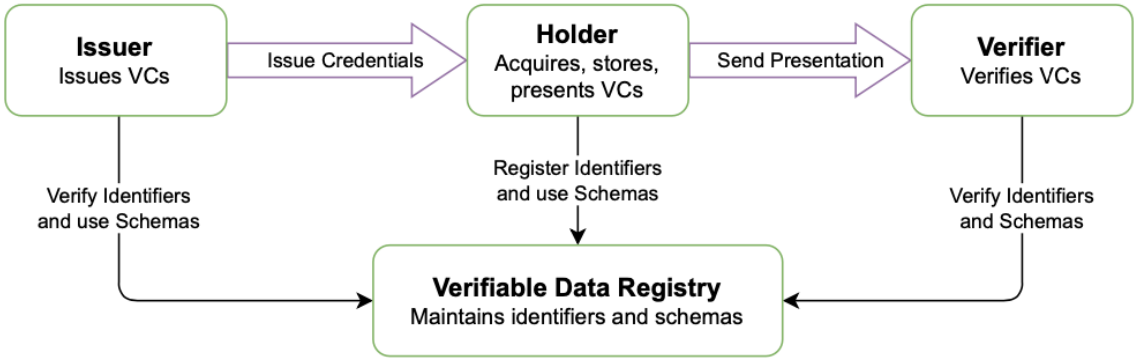
- **Global Standardization:**
  - Organizations like **W3C** and the **Decentralized Identity Foundation (DIF)** are standardizing DIDs and VCs for interoperability.
- **Regulatory Support:**
  - SSI aligns with GDPR by ensuring **privacy by design** and user control.
  - eIDAS2 provides a unified framework for cross-border identity services.
- **Collaboration for Interoperability:**
  - A **unified European approach** through eIDAS2 fosters secure and seamless digital interactions.

Core Components of SSI: DIDs and VCs

- **Decentralized Identifiers (DIDs)**:
  - Self-generated, unique identifiers independent of centralized registries.
  - Resolvable through decentralized systems for secure verification.
- **Verifiable Credentials (VCs)**:
  - Cryptographically signed digital statements issued by trusted entities (e.g., governments, universities).
  - **Features**:
    - Tamper-proof and verifiable without contacting the issuer.
    - Privacy-preserving through selective disclosure.

VC Issuance and Verification Process

- **Issuance Process:**
  1. Issuer uses the holder's DID to create and sign the VC.
  2. VC is stored in the holder's digital wallet.
- **Verification Process:**
  1. Holder presents the VC to a verifier.
  2. Verifier validates the VC using the issuer's public key.
- **Revocation and Updates:**
  1. **Status Lists:** Enable verifiers to check if a credential is still valid.
  2. **Blockchain:** Stores immutable records of credential revocation or updates.



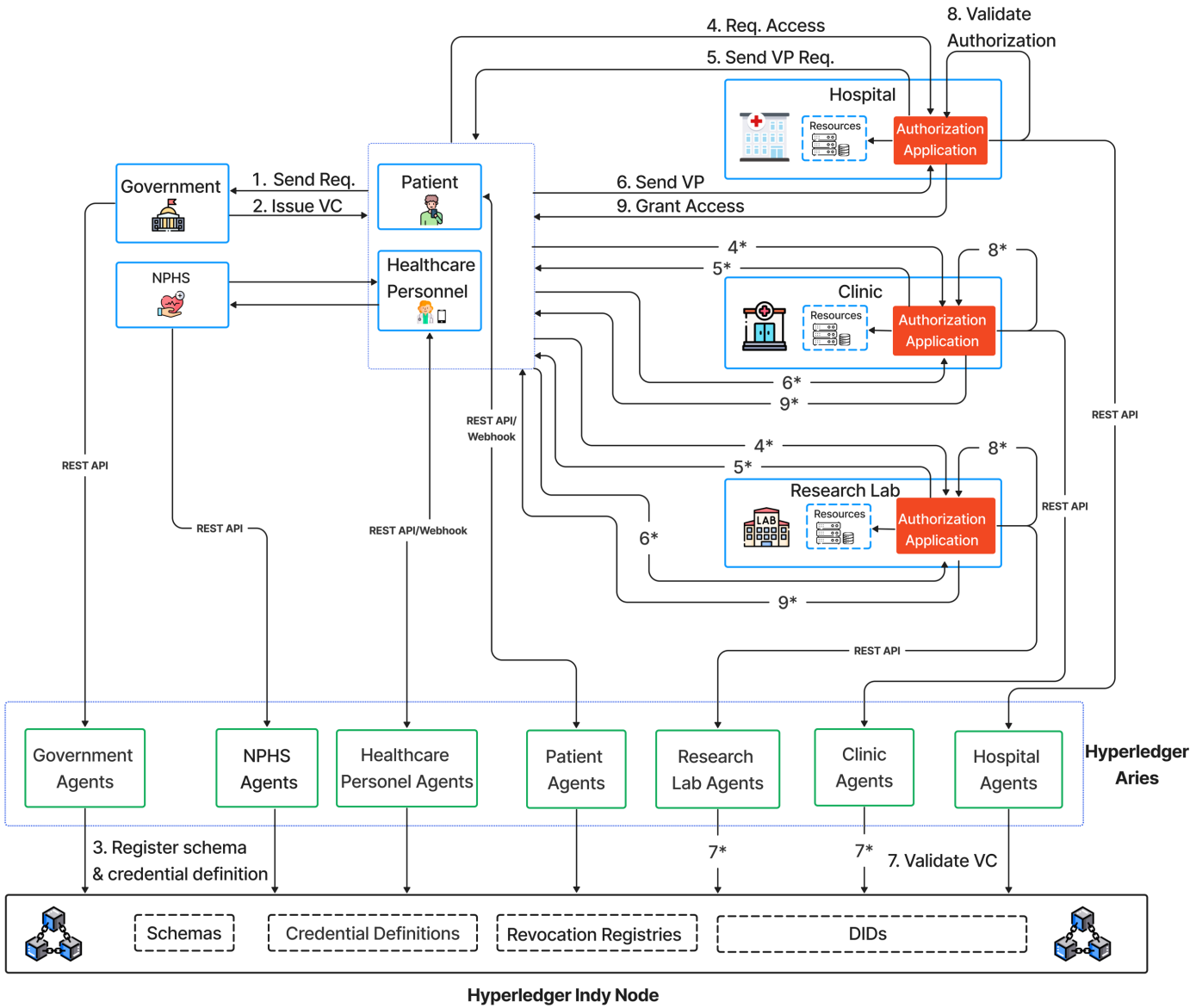
Source: https://www.w3.org/TR/vc-data-model-2.0/

Privacy-Preserving Techniques in SSI

- **Zero-Knowledge Proofs (ZKPs):** A cryptographic method that enables proving a statement without revealing the underlying data. (**Example:** Proving over-18 status without disclosing birthdate.)
  - **Key Features:**
    - Protects sensitive information.
    - Non-interactive ZKPs streamline verification.
- **Selective Disclosure:** Enables users to share specific attributes from VCs while keeping other details private.
  - **Techniques:**
    - **BBS+ Signatures:** Allow sharing only the required attributes.
    - **Merkle Trees:** Efficiently organize and prove specific data elements.
- **Benefits:**
  1. Aligns with **GDPR** principles of **data minimization** and **privacy by default**.
  2. Enhances user trust in secure and private digital interactions.
  3. Protects sensitive information across sectors.

SSI in Healthcare: Empowering Patients

- SSI allows patients to have **direct control over their medical records** and securely share them with healthcare providers.
- **Key Use Cases:**
  1. **Patient-Controlled Records:**
     - VCs issued by healthcare providers, e.g., vaccination records, prescriptions.
     - Patients decide who can access specific records.
     - DIDs are used for secure identification without revealing unnecessary details.
  2. **Secure Sharing of Medical Data:**
     - **Example:** Sharing COVID-19 test results using a VC.
     - Patients can prove test results without revealing additional sensitive information.
- **Benefits:**
  - **Data Privacy:** Patients share only what is necessary, reducing over-disclosure.
  - **Interoperability:** Enables secure sharing across healthcare systems.
  - **Regulatory Compliance:** Aligns with GDPR principles like data minimization and privacy by design.



Decentralized Identity Management for Healthcare Systems

Source: https://arxiv.org/pdf/2307.16239

SSI in IoT - Device Authentication

- **Internet of Things (IoT) Use Case:**
  - **DIDs** are assigned to IoT devices to provide a unique identity for each device.
  - Enables **peer-to-peer authentication** without centralized registries.
- **Secure Data Exchange:**
  - Devices use **VCs** to prove their identity, ensuring that only trusted devices communicate within an IoT network.
  - **Data Integrity:** Information exchanged between devices is encrypted, preventing unauthorized interception.
- **Benefits:**
  - **Security:** Reduces risks of unauthorized access to the IoT ecosystem.
  - **Scalability:** The decentralized approach supports millions of devices without the bottlenecks of a central authority.

Financial Services Use Case - Decentralized Finance (DeFi)

- **Scenario:** Using SSI to access a decentralized finance platform.
- **Authentication:**
  - Users authenticate using their **DID** and provide **Verifiable Credentials** to prove eligibility (e.g., proof of age, identity).
- **Integration with Smart Contracts:**
  - Smart contracts interact with DIDs to verify user identity and eligibility without manual intervention.
- **Benefits:**
  - **Privacy-Respecting Transactions:** Users maintain anonymity while fulfilling KYC requirements.
  - **Compliance and Security:** SSI helps DeFi platforms comply with regulatory requirements while minimizing user data exposure.

Government Services - Digital Citizenship and E-Voting

- **Digital Citizenship:**
  - Governments issue digital IDs as VCs, enabling citizens to securely access public services such as **healthcare** and **taxation**.
  - **Interoperability:** The same DID can be used across government services, allowing secure and unified access.
  - **User Control:** Citizens decide which government departments can access their personal information, ensuring GDPR compliance.
- **E-Voting:**
  - Citizens use digital voter IDs to vote online securely.
  - **Privacy Assurance:** Voters' eligibility is verified without compromising anonymity, maintaining confidentiality.
  - **Process:**
    1. Citizens receive digital credentials from the government.
    2. Credentials are used to access e-voting portals securely.
    3. Verifiers authenticate voter eligibility without linking votes to identities.
- **Benefits:**
  - **Transparency in Elections:** Improved voter trust and accountability.
  - **Simplified Access:** A unified digital ID can be used for various public services.

Government Services Use Case - Border Control with SSI

- **Challenge:** Traditional passport verification involves manual checks and central databases, which can be slow and prone to errors.
- **Scenario:** Using SSI for secure and efficient border control.
- **Traveler Authentication:**
  - Travelers present VCs issued by their home country through a digital wallet.
- **Verification Process:**
  - Border control officers verify the VC using cryptographic validation without accessing the full identity document, maintaining privacy.
- **Privacy-Preserving Data Sharing:**
  - Only relevant travel details are shared with authorities, minimizing exposure of sensitive data.
- **Benefits:**
  - **Speed and Efficiency:** Faster processing compared to manual passport checks.
  - **Privacy:** Only necessary information (e.g., visa status or passport validity) is shared.
  - **Enhanced Security:** Border checks are less likely to be manipulated, improving overall security.
  - **Cross-Border Interoperability:** Travelers can use the same credentials across jurisdictions, eliminating the need for multiple documents.

SSI Security Challenges and Mitigation

- **Preventing Identity Theft:**
  - **Decentralized Control:** Eliminates centralized databases, reducing the risk of mass breaches.
  - **Multi-Factor Authentication (MFA):** SSI wallets support MFA for enhanced security.
  - **Biometric Authentication:** Adds an extra layer of protection using fingerprints or facial recognition.
- **Data Breach Mitigation:**
  - **Decentralized Storage:** Avoids centralized databases, minimizing large-scale breaches.
  - **Encryption:** Protects sensitive data during storage (data-at-rest) and transfer (data-in-transit).
  - **Controlled Access:** Users determine which verifiers can access their data, ensuring limited exposure.
- **Credential Revocation and Recovery:**
  - **Revocation Mechanisms:**
    - **Status Lists:** Allow verifiers to check if a credential is valid or revoked.
    - **Blockchain-Based Revocation:** Provides a tamper-proof record of credential status.
  - **Recovery Protocols:**
    - **Social Recovery:** Trusted contacts help recover credentials if access is lost.
    - **Seed Phrases:** A fallback method to regain wallet access.
- **Benefits of SSI Security:**
  - **Resilience:** Users maintain control even in case of device compromise (aligns with NIS2 requirements for critical sectors).
  - **Enhanced Privacy:** Reduces reliance on centralized authorities, mitigating threats of mass exposure.

Phishing and Social Engineering Resistance in SSI

- **User-Centric Authentication**:
  - **SSI Wallets**: Wallets are used to authenticate interactions, eliminating the need for usernames and passwords, which are often targeted in phishing attacks.
  - **No Password Reuse**: SSI avoids passwords, eliminating risks associated with phishing emails aimed at collecting login credentials.
- **Visual Security Indicators**:
  - **Trusted UI**: SSI wallets display recognizable indicators that help users validate legitimate requests, reducing susceptibility to phishing.
- **Machine Learning-Based Anomaly Detection**:
  - Detects unusual or suspicious interactions, adding an extra layer of security against social engineering attacks.

Education and User Empowerment in SSI

- **User Education - A Crucial Factor:**
  - Users must understand key management, credential handling, and secure sharing.
  - Without proper knowledge, privacy and control can be compromised.
- **User Onboarding Best Practices:**
  - Simplify SSI wallet usage with onboarding guides that explain how to manage credentials and maintain privacy.
- **Continuous Security Awareness:**
  - **Education Programs:** Teach users about the importance of maintaining control over private keys and avoiding phishing.
  - **Interactive Tutorials:** Provide simulated use cases to help users understand scenarios involving the use of SSI.
- **Gamification of Security Training:**
  - Use interactive elements, such as quizzes and rewards, to engage users in learning best practices for secure SSI use.

Emerging Trends and Research Directions in SSI

- **Quantum-Resistant Cryptography:**
  - Developments in quantum-resistant algorithms are essential to ensure that SSI cryptography remains secure against quantum computing threats.
- **Artificial Intelligence in SSI:**
  - AI could be used to analyze transaction data and detect fraudulent behavior in SSI-based identity systems, enhancing security.
- **SSI for Edge Computing and 5G/6G:**
  - With the rise of **5G** and **edge computing**, SSI can provide secure authentication for billions of edge devices, ensuring their unique identities and safe communication.
- **Standardization Efforts:**
  - Global initiatives to standardize **DIDs**, **VCs**, and interoperability protocols are underway, helping establish a unified approach to digital identity management.

Challenges Facing SSI Implementation

- **User Adoption:**
  - **Complexity:** The concept of decentralized identifiers and digital wallets is still new to many users, requiring significant education.
  - **Trust:** Users must trust the SSI technology to store and manage their personal information securely.
- **Interoperability:**
  - Ensuring that **DIDs** and **VCs** issued in one jurisdiction or network are recognized across others remains a challenge, requiring standards and protocols to be widely adopted.
- **Scalability:**
  - **Blockchain Limitations:** SSI relies on decentralized ledgers, which need to be scalable to handle millions of transactions.
  - **Cost of Transactions:** Using public blockchains can introduce transaction costs, making it expensive for mass adoption.
- **Regulatory Barriers:**
  - SSI must comply with varying regulations across countries, and achieving global regulatory alignment is challenging.

SSI and Digital Sovereignty

- **Digital Sovereignty:** The ability of individuals and nations to have control over their digital presence and data, independent of external control.
- **SSI as an Enabler:**
  - **User Control:** SSI empowers users to manage their digital identity, which aligns with the principles of digital sovereignty.
  - **Decentralized Infrastructure:** Avoids dependency on centralized authorities, enabling governments and organizations to regain control over digital services.
- **National-Level Initiatives:**
  - **eIDAS2 in Europe:** An example of digital sovereignty in action, where European citizens use digital wallets to manage identity across borders, reducing dependency on third-party tech giants.
- **Alignment with EU Policies:**
  - The EU's focus on privacy, data security, and independence is strongly supported by SSI's framework.

Digital Sovereignty in Norway

- In Norway, we submitted a proposal to establish a research and innovation center: **Norwegian Center for Digital Sovereignty (NCDS)**.

- The first **International Conference on Digital Sovereignty (ICDS)** will be held 28-30 November 2024 in Oslo.

Future of SSI - Adoption Challenges

- **User Education and Awareness:**
  - Managing digital identity is a new concept for many users. Clear onboarding and training materials are essential for ease of adoption.
  - Trust in the technology must be built to enable widespread acceptance.
- **Interoperability Standards:**
  - The success of SSI depends on universally accepted standards. Organizations like W3C are working to standardize DIDs and VCs.
- **Cost and Scalability:**
  - Blockchain can be costly for large-scale SSI systems. Scalable solutions like layer-2 protocols help reduce costs and improve efficiency.
- **Integration with Legacy Systems:**
  - Adapting existing infrastructure to work with SSI requires collaboration among governments, tech firms, and financial institutions to ensure seamless interoperability.

Roadmap for SSI Implementation

- **Global Standards:**
  - Accelerate the adoption of standardized DIDs and VCs through global efforts led by W3C and other organizations.
  - Ensure interoperability by aligning international standards with regulatory frameworks like GDPR, eIDAS2, and NIS2.
- **Collaborative Governance:**
  - Foster partnerships among governments, industries, and non-profits to create unified policies and regulatory support for SSI.
  - Promote cross-border regulatory alignment to facilitate uniform SSI adoption.
- **Scalable and Secure Technology:**
  - Develop quantum-resistant cryptographic standards to secure SSI against future threats.
  - Implement layer-2 scaling solutions (e.g., rollups) to reduce costs and improve transaction efficiency for blockchain-based systems.
- **Mass Adoption Enablement:**
  - Design user-friendly SSI wallets to accommodate users with diverse technical skills.
  - Launch user education and training programs to build trust and promote widespread SSI adoption.

Ongoing Projects

1. **Co-created Health Technology (CoTecH)**
   - Duration: May 2022 - Apr. 2028
   - Funded by Research Council of Norway

2. **Decentralized Privacy-Preserving Sharing of Health Data (DeHelse)**
   - Duration: Jan. 2024 - Dec. 2024
   - Funded by Regional research funds (RFF)

3. **Cybersecurity for Critical Infrastructure**
   - Duration: Jan. 2025 – Dec. 2028
   - Funded by Norwegian Directorate for Higher Education and Skills (HKDir) (UTFORSK)

Interested in Collaboration? Let's Connect!

Conclusion

- **User Empowerment:** SSI puts users in control of their digital identities, ensuring autonomy, privacy, and trust while reducing dependence on centralized authorities.
- **Transformative Potential:** SSI is driving secure and efficient identity solutions across critical sectors like healthcare and government services, enabling patient-controlled data sharing and fraud-resistant identity verification.
- **Future Outlook:** With advancements in cryptography and standards, SSI will redefine digital identity with a secure and interoperable ecosystem.

Thank you!

ANY QUESTIONS?

Email: mohsen.toorani@usn.no

LinkedIn: toorani