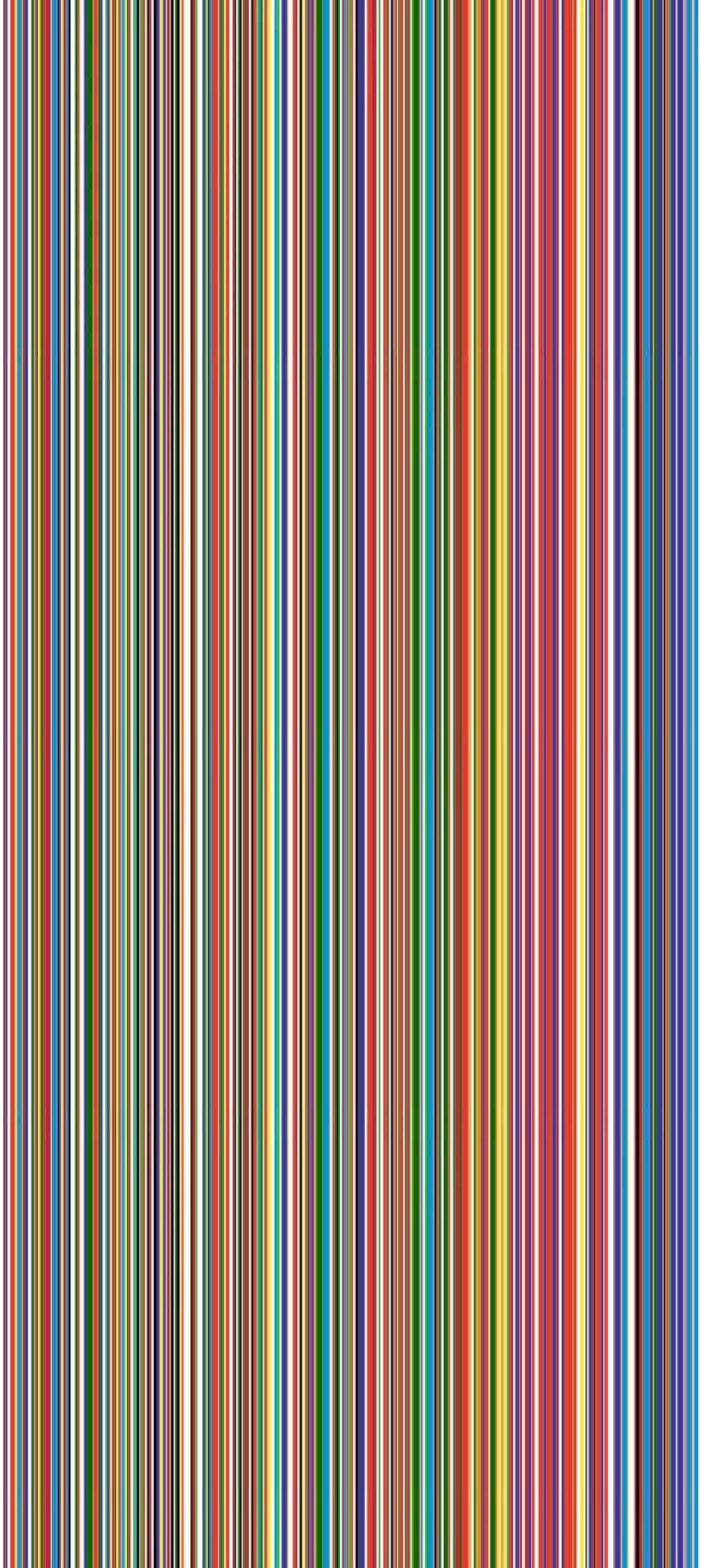


Global Digital Collaboration

Geneva July 2025

Book of Proceedings

Foreword

At the heart of the Global Digital Collaboration Conference 2025 (GDC25) lies a simple yet profound conviction: collaboration is not merely a theme of our work - it is its very foundation. It is embedded in our mission, reflected in our approach, and even carried in the name of this gathering. In a world where digital systems shape the daily lives of billions, no single actor, public or private, can build the future alone. True progress requires trust, openness, and collective leadership that only genuine collaboration makes possible.

The idea for this conference traces back to a conversation sparked by Daniel Goldscheider, whom many early participants jokingly referred to as the “father” of GDC25. Daniel himself was quick to respond that GDC25 has never been, and must never become, the product of a single individual or organisation. GDC25 has many parents. Indeed, 51 organisations stepped forward as Co-organisers of the inaugural edition, shaping GDC25 from its earliest concept into the platform it is today. Their enthusiasm and shared sense of purpose transformed a vision into action with remarkable speed.

That speed was put to the test immediately. The very first meeting among the core organisers, where they asked themselves whether it would even be feasible to convene a global community so quickly, took place just fifteen weeks before the conference, in March 2025. What followed was an extraordinary demonstration of dedication. Over those fifteen weeks, and especially during the final stretch, the team worked with relentless intensity, fuelled by the belief that a global conversation on digital collaboration could not wait. Many nights were short; some had no sleep at all. Yet the commitment of dozens of individuals and institutions made the impossible achievable.

This Book of Proceedings serves as a record of that collective achievement. It distils the insights, debates, visions, and practical proposals that emerged across the three days of GDC25. It is designed not only for those who were able to attend in person, but also for the wider international community that follows and contributes to this work. Our hope is that these reflections provide both a reference and an inspiration for the many steps that lie ahead.

Finally, we extend our deepest gratitude to the Sponsors - Google, Huawei, Mastercard, and Visa - and Co-organisers of GDC25. Their support, financial and intellectual, made this conference possible. GDC25 stands on their contributions, and its future will continue to be shaped by their leadership. Last but not least, we would like to thank the team of Trust Square for their wonderful job in terms of logistics and hospitality.

Together, we have begun something meaningful. Together, we will continue it.

Rolf Rauschenbach
Deputy Head e-ID-Unit and Communications Officer e-ID
Federal Office of Justice FOJ
Swiss Confederation

Table of Content

About GDC25

The Global Digital Collaboration Conference 2025 (GDC25) was initiated to foster collaboration on specific topics that require the involvement of multiple actors and organisations to succeed. By bringing together key stakeholders, the conference aimed to facilitate effective dialogue around digital identity and collaboration frameworks. The two-day conference, held in Geneva, Switzerland, in July 2025, gathered more than 1'000 participants from around the world.

For this edition, the main goals were centred on two key objectives:

- Advancing Global Interoperability: Sessions focused on a) global interoperability, defined as the ability to exchange personal and other data safely, securely, and seamlessly across the worldwide web; and subsequently b) the development of unified standards that are global, inclusive, and consensus driven.
- Fostering Comprehensive Collaboration: Discussions were designed to draw participants out of traditional silos, merging perspectives from typically separate communities to enhance cooperation among diverse stakeholders.

To achieve these goals, GDC25 brought together an unprecedented number and diversity of ecosystem organisations in a multi-stakeholder format. As many of these organisations had never convened before, the conference represented a milestone in collaborative governance. In fact, while hosted by the Swiss Confederation, GDC25 was co-organised with 51 diverse organisations, including UN bodies, international organisations, standardisation bodies, and open-source communities (see *Annex 1* for the full list). Being united by the goal of advancing interoperability, these Co-organisers were instrumental in defining both the scale and mission of the event: They actively shaped the agenda and session content through a participatory process. Notably, corporate sponsors (Google, Huawei, Mastercard, and Visa) were not guaranteed speaking slots; they could only present if nominated by one of the Co-organisers. This approach exemplified the inclusive and collaborative nature of GDC25, particularly reflected on the second day, which focused on active engagement and co-creation among attendees.

GDC25 was structured as follows:

- Day 1: Designed to give participants an overview of current projects and discussion, featuring 22 sessions (see *Recap Day 1 – Plenary Sessions*).
- Day 2: Inspired by the unConference (Open Space Technology) format, featuring approximately 100 sessions proposed by Co-organisers ahead of GDC25 (see *Recap Day 2 - Collaborative Sessions*).

The following Book of Proceedings provides insights and key outcomes from both days.


Global Digital Collaboration Conference 2025
OECD
UNECE
WORLD BANK GROUP
IEC
IFRC
ISO
CENELEC
DIF
ETSI
fido ALLIANCE
Global Platform
OpenID
W3C
ECLIPSE FOUNDATION
FINOS
OPEN MOBILE HUB
OpenWallet FOUNDATION
Tazama
AAMVA
ayra
BGIN
DCC
digital impact alliance
DIDAS
DIGITAL SOCIETY
FIDES.
Accelerating Digital Trust
GLEIF
MOSIP
Project Liberty Institute
Verifiable.Trade
Google
HUAWEI
VISA
GC 25

Recap Day 1 – Plenary Sessions

Day 1 aimed to provide comprehensive coverage of the digital collaboration landscape through keynote speeches, panels and use case showcases: The morning was structured as a "world tour", featuring presentations organised in geographic terms. The afternoon focused on specific use cases, including travel credentials, health credentials, driver's licenses, and car keys. The following sections recap the sessions from Day 1[1].

Global Patterns and Regional Contexts

Digital Identity Wallet: A Cornerstone of Europe's Digital Public Infrastructure

Category: Europe I **Panellists:** Norbert Sagstetter (European Commission), Florent Tournois (ANTS), Pramod Varma (CDPI), Michael Butz (ESD), Carsten Rosche (Germany) I **Co-organisers:** European Commission I **YouTube:** Link

The panel discussion examined the European Digital Identity (EUDI) Wallet as the core of Europe's Digital Public Infrastructure, addressing the critical tension between high security and broad inclusivity. The EUDI Wallet initiative aims to set global standards for identity, establishing a regulatory obligation for all EU member states to issue the wallet to citizens by the end of 2026. The wallet will be accepted in both public and private sectors wherever high-assurance identification is required, maintaining strict security and privacy orientation with users having complete control over which data and credentials they share. Furthermore, it is envisioned to serve as the core of European digital public infrastructure, linking identity, data exchange, and payments in a trusted and secure manner whilst enabling inclusion and digital citizenship. The new framework represents a substantial advancement because it focuses on the entire ecosystem rather than identity alone, harmonising fragmented standards and protocols.
The panel extensively discussed the fundamental conflict between security and inclusivity, emphasising lessons from large-scale implementations serving over a billion users. Current implementation approaches vary across member states, with some pursuing very high security levels that result in low inclusion, whilst models requiring one person, one device, one app, one identity create barriers for common scenarios such as family members assisting relatives with e-government services. The architectural approach being developed intentionally accommodates users across the economic spectrum, recognising that most daily transactions do not require the highest assurance levels and pragmatic solutions should provide appropriate security for each context. The session concluded with consensus that effective digital wallet implementation requires balancing security with inclusion, reducing transaction costs whilst expanding access to essential services, and building systems that reflect democratic values through international collaboration, open standards, and user-centric design principles.

Digital Identity Wallet: Public Private Partnerships

Category: Europe I **Panellists:** Alan Stapelberg (Google), Norbert Sagstetter (European Commission), Pramod Varma (CDPI), Thomas Kostka (Savingsbank) I **Co-organiser:** European Commission I **YouTube:** Link

This panel examined how public-private partnerships are essential for building effective digital identity infrastructure. Success requires combining public sector strengths, namely trust, confidence,

1 Please note, the recaps have been produced and shortened using AI tools to summarise the respective session recordings uploaded to YouTube.

and security with private sector capabilities in customer orientation, technology innovation, and ease of use. The private sector contributes through developing open platforms and wallet solutions, creating standardised APIs that allow relying parties to connect with multiple wallets through a single interface, and building compelling use cases that demonstrate the value of digital credentials. Key innovations include zero-knowledge proof technology for privacy-preserving age verification, which has been open-sourced to advance industry-wide progress. Financial institutions occupy a unique position as trusted intermediaries, leveraging existing know-your-customer infrastructure to offer supplementary identity services alongside government eID systems. Banks are launching digital age verification services that integrate with credential management platforms and privacy-enhancing technologies, enabling seamless, one-click age checks without revealing personal data. The regulatory framework actively supports this model, permitting private sector wallet issuance under government control and certification. By piloting real-world solutions now, organisations can shape emerging standards within evolving digital identity frameworks whilst maintaining the essential balance between innovation and oversight that characterises successful public-private collaboration.

EWC and WE BUILD: Two consortiums - one vision

Category: Europe I **Speaker:** Rob Brand (WE BUILD) I **Co-organiser:** European Commission I **YouTube:** Link

Two EU digital wallet consortiums are presented, namely EWC and WE BUILD, which share the vision that wallets are crucial for a sustainable, real-time digital economy. Both are use case-driven, based on the eIDAS regulation and Architecture Reference Framework, and work towards achieving interoperability whilst providing feedback to the Commission. EWC, initiated by the Swedish business register and now nearly complete, achieved significant milestones including the first real payment transaction using a wallet, developed a rulebook for legal person identification data, and successfully piloted business use cases such as hotel registration and airline check-in. Building on this success, WE BUILD, led by the Dutch Ministry of Economic Affairs and business registers from the Netherlands and Sweden, represents a substantial expansion with 181 organisations across 22 member states, focusing on payments, supply chain, and business use cases. WE BUILD encompasses the entire ecosystem including business registers, verifiable credential issuers, relying parties, wallet providers, QTSPs for electronic signatures, and technology providers, integrating results from EWC, NOBID, and POTENTIAL consortiums alongside the Commission's business wallet initiative. The consortium officially launched on 3 September with a 24-month timeline to establish a fully functioning ecosystem.

The NOBID Consortium from North to South and East to West

Category: Europe I **Speaker:** Tor Alvik (NOBID Consortium) I **Co-organiser:** European Commission I **YouTube:** Link

The presentation outlined experiences from one of the large-scale pilots working on the EU digital wallet, a geographically diverse consortium spanning from Iceland to Italy that reflects Europe's varied payment and banking landscape, encompassing entities ranging from those with employee numbers matching Iceland's entire population to much smaller operations. Initially focused on payments whilst exploring banking-related use cases, the consortium operates as a public-private endeavour balancing member states' legislative obligations to implement core wallet functionality, including authentication, signing, and the significant challenge of onboarding 400 million users at high security levels, with practical use case development by payment scheme actors and experienced wallet designers. Extensive collaboration, including an advisory board for European payment actors and close alignment with other consortia, achieved a common understanding of wallet-based payments

and successfully harmonised solutions across Europe, with developed wallets notably exhibiting the intended similarity.
Ongoing work with the Commission, along with successful testing of payment processes and remote signing functionality built on existing electronic identification methods, demonstrates that the large-scale pilot approach effectively develops requirements through practical collaboration. Partners will continue this work in the next round of pilots across subsequent consortia, with expectations that payment functionality in the European wallet will be realised in the near future.

Digital Credentials for Europe - DC4EU LSP

Category: Europe I **Speaker:** Dr. Ignacio Alamillo-Domingo (DC4EU - LSP) I **Co-organiser:** European Commission I **YouTube:** Link

The Digital Credentials for Europe Large Scale Pilot (DC4EU LSP) demonstrated how the European digital identity wallet can transform data sharing by returning control to citizens and overcoming longstanding interoperability limitations. The project involved approximately 100 entities testing strict regulatory requirements across educational qualifications and social security use cases, most notably the European Health Insurance Card for millions of citizens. Its unique contribution was developing a hybrid trust model that combines the regulatory wallet framework with blockchain technology from the European Blockchain Service Infrastructure, using distributed ledgers as verified data registries to complement information from regulatory authorities. This approach enables credential verification both within and beyond EU boundaries, which is essential for international contexts. Four key lessons emerged: the wallet effectively transforms how public sector bodies share data as authentic sources; many potential issuers cannot afford expensive qualification or notification processes as qualified trust service providers or notified bodies; a hybrid approach combining classical and decentralised public key infrastructure protects users whilst enabling broader participation and international verification of non-regulated information; and connecting with global identity federations is essential for worldwide usability.

Large Scale Pilot presentation

Category: Europe I **Speaker**: Florent Tournois (POTENTIAL) I **Co-organiser**: European Commission I **YouTube:** Link

The large-scale consortium comprising 19 countries, 161 public and private partners, and 58 observers worked collaboratively to establish the groundwork for the European Digital Identity Wallet, organised primarily around member state administrations to address sovereignty issues and personal identity concerns. Following approximately one year of specification work whilst awaiting the European Commission's reference implementation, the consortium organised a series of interoperability testing events that used compatibility matrices to ensure technical integration between country wallets, relying parties, and other components, ultimately demonstrating six key use cases: e-government services access, bank account opening, SIM registration, mobile driving licence (for car rental and checks), qualified electronic signature, and e-prescription. This successful demonstration established the wallet as a viable practical concept and prompted transition to a successor consortium with a more citizen-oriented focus, which is now developing travel-related use cases, contributing to mobile driving licence normalisation through vehicle registration certificates, and incorporating strong customer authentication at payment points with input from other European consortia.

China-Singapore-Hong Kong Cross-border Decentralized Identity and Credential Trials and Use Cases

Category: Asia & Oceania I **Speakers:** Priscilla Chen (Singapore IMDA), Yifan He (Red Date Technology) I **Co-organiser**: OpenWallet Foundation I **YouTube:** Link

The presentation addressed Singapore's digital identity infrastructure and a cross-border verifiable credentials pilot programme involving Singapore, China, and Hong Kong. Singapore operates a four-pillar digital utility stack comprising centralised digital identity systems for individuals and corporations, verifiable credentials for document attestation, data exchange infrastructure, and digital payments. Whilst the centralised system serves high-security use cases in finance, healthcare, and government services, verifiable credentials are being explored to complement this infrastructure by addressing privacy concerns and enabling private sector data sharing beyond government-held information. The initiative aims to transition domestic standards to become globally compliant and W3C-compatible, supporting medium to low-security use cases where users prefer decentralised verification without government oversight of every transaction.
The sandbox pilot demonstrates a multi-issuer platform extending existing government identity infrastructure, with verifiable data stored on public blockchain whilst personal information remains encrypted off-chain. This architecture enables universal verification without connecting to government systems, shifting control from government to identity holders whilst reducing costs and expanding the verifier base. The three-phase exploration encompasses streamlining access management through digital wallets, improving electronic know-your-customer processes to prevent fraud, and enhancing cross-border interoperability. Practical applications include linking cryptocurrency wallets to government identity through zero-knowledge proofs, and automating online form completion with pre-verified credentials, among others. This represents a fundamental shift from human-readable physical documents to machine-readable cryptographic data, enabling faster processing whilst enhancing privacy through encryption and selective disclosure capabilities.

Digital Identity Innovation in Korea: Public-Private Collaboration for Scalable and Secure Wallet Solutions

Category: Asia & Oceania I **Speakers:** Sanghwan Park (Korea Internet & Security Agency KISA), Ace Shim (Hopae), Wonsoek Baek (Samsung Electronics)I **Co-organisers:** ITU, OpenWallet Foundation I **YouTube:** Link

South Korea has established a comprehensive digital identity framework built on three pillars: electronic signature certification, online identity verification services, and blockchain-based decentralised identity services protecting user privacy in the Web 3.0 environment. Since 2018, 119 pilot projects have been supported across areas including online voting and central bank digital currencies, informing plans for digital wallet guidelines and fundamental blockchain legislation. Key implementations demonstrate two successful models: public-led innovation, for example where government agencies developed mobile driver's licences and resident registration cards with full legal validity; and private-led innovation, for example a COVID-19 vaccination certificate system that was downloaded 43 million times. The pandemic response achieved global interoperability with the EU and Singapore through integration of national passport databases, WHO data standards, and diplomatic policy agreements, with the wallet technology subsequently deployed across IT and telecommunications platforms to generate an additional 80 million wallets. The success of digital identity initiatives proved crucial in enabling Samsung Electronics to transition its payment service to a comprehensive digital wallet platform in 2024, demonstrating how public-private collaboration and regulatory sandbox systems can drive widespread adoption of innovative digital services.

Australian Verifiable Credential Journey

Category: Asia & Oceania I **Speakers:** Christopher Goh (Austroroads), Arjan Geluk (A4 Advisory), Konstantin Papaxanthis (Scytales) I **Co-organiser:** Austroads I **YouTube:** Link

Australia's national initiative adopt the Mobile Driving License (MDL) and Verifiable Credentials (VCs), emphasizing a policy framework built on both regulatory safety and the need to preserve dignity and provide service accessibility for vulnerable populations. Whilst identity verification is largely solved, the real friction lies in proving eligibility for services and linking them to payment. Australia has adopted ISO 18013 and 23220 standards, successfully demonstrating real-time cross-border verification between three countries, the European reference wallet, four American states, and five Australian jurisdictions. The implementation uses device retrieval rather than server retrieval, with biometric binding during enrolment, and emphasises selective disclosure and zero-knowledge proofs to verify statuses without revealing underlying data. The biggest adoption challenge lies with relying parties, addressed through integration into point-of-sale payment devices to eliminate additional equipment costs. Nearly all Australian states and territories aim to deploy ISO-compliant mobile driving licences within 18 months, with immediate focus on engaging relying parties, regulators, banks, and industry bodies to drive acceptance.

Global South Innovations in DPI

Category: Africa, Latin America & Caribbean I **Panellists:** Armando Manzueta (Dominican Republic), Pramod Varma (CDPI), Julia Clark (WBG) I **Co-organisers:** CDPI, World Bank Group I **YouTube:** Link

Digital Public Infrastructure (DPI) development across the Global South was explored through examples from India and the Dominican Republic, with the World Bank supporting over 70 countries on digital ID and 50 on government-to-person payments. India's journey demonstrates transformative potential: starting from a high-cost, low-trust environment where less than 20% had bank accounts in 2010, the implementation of open, interoperable digital rails enabled 1.4 billion people to obtain digital ID (used 70-80 million times daily), created 10 billion verifiable credentials, and increased domestic capital market participation from under 2% in 2016 to 14% by 2024. The Dominican Republic, at an earlier stage, has established a national interoperability framework adapted from Estonia's XRO platform, launched authentication systems and a digital wallet supporting verifiable credentials, with future priorities including payment infrastructure for financial inclusion. Key principles emphasised include ensuring Global South countries participate as co-creators rather than observers in standard-setting bodies, maintaining interoperability to prevent digital systems from hindering cross-border movement of money and information, and enabling private sector diversity and choice whilst governments focus on specifications and compliance standards. Further, they should define digital society building blocks, shift from vendor-specific procurement towards capacity-building ecosystems, and position government as an enabling platform upon which local innovators and startups can build extended services.

Regulatory Approach for Implementing Digital ID under REAL ID in U.S.

Category: North America I **Speaker:** George Petersen (Transportation Security Administration) I **Co-organiser:** OpenWallet Foundation I **YouTube:** Link

The US Transportation Security Administration adopted an innovative regulatory approach for implementing digital IDs and mobile driver's licences under the Real ID Act, legislation passed following 9/11 to improve identity assurance across 56 US licensing jurisdictions covering over 280 million driver's licences and ID cards. Facing the challenge that traditional US rulemaking processes take five to seven years whilst digital ID technology was rapidly innovating with immature standards,

risking states developing incompatible solutions, TSA adopted a multi-phase approach prioritising stakeholder engagement and transparency. Beginning with a Request for Information in April 2021 rather than immediate formal rulemaking, they conducted intensive collaboration with states, industry, and privacy advocates through the American Association of Motor Vehicle Administrators, holding regional meetings and roundtables to incorporate feedback. This strategy proved remarkably successful: the Notice of Proposed Rulemaking was published in August 2023 (less than two years after the RFI), received only 31 comments which were all addressed, and the final rule was published in October 2024 (just one year later). The regulations establish minimum standards for security, privacy, and interoperability whilst remaining technology-neutral, allowing any digital ID solution meeting these requirements through certification processes, thus facilitating innovation, investment, and international interoperability. Currently, 15 US states operate mobile driver's licence programmes under this framework.

The Swiss e-ID and trust infrastructure

Category: Europe I **Speakers:** Rolf Rauschenbach (Federal Government), Daniel Säuberli (DIDAS), Pascal Mainini (Digital Society) I **Co-organisers:** Swiss Confederation, DIDAS, Digital Society I **YouTube:** Link

Switzerland's electronic identity (e-ID) project represents a significant political and technical evolution following the 2021 referendum that rejected the original proposal with over 64% opposition due to concerns about private sector involvement, centralisation, and privacy. The revised e-ID 2.0 addresses these criticisms through a state-issued, voluntary system built on self-sovereign identity principles with privacy-by-design architecture, including DID:web identification, SD-JWT verifiable credentials, and innovative batch issuance ensuring unlinkability between presentations. Beyond the e-ID itself, Switzerland is developing an open trust infrastructure designed to reflect its federal structure, supporting three ambition levels: the basic e-ID, government credential issuance (such as driver's licences by cantons), and a fully open ecosystem where any national or international organisation can participate as issuers or verifiers using third-party wallets and flexible governance models. With a budget of CHF 180 million over five years and Public Beta, the public test environment with the swiyu Wallet, already available, the project faces a binding referendum on 28 September 2025 that will determine whether it proceeds. Ongoing challenges include developing organisational identity solutions for cross-jurisdictional interoperability and educating organisations beyond the technical community about the infrastructure's potential for enabling user-centric services, fraud prevention, and automated workflows with machine-readable data.

Cross-Border Interoperability - Insights From the G7 Mapping Exercise of Digital Identity Approaches

Category: Global I **Panellists:** Anthony Carmoy (France Titres), Cecilia Emilsson (OECD), Connie Lasalle (NIST), Dr. Charlie Smith (OfDIA) I **Co-organisers:** OECD, LSPs I **YouTube:** Link

The session focused on cross-border digital identity interoperability and presented insights from a G7 mapping exercise of digital identity approaches, conducted under the Italian G7 presidency and supported by the OECD. The mapping involved G7 countries, the United States, United Kingdom, Italy, France, Germany, Japan, and Canada, along with the European Commission. The goal of this small, intentional exercise was to establish a common understanding and mapping of digital identity frameworks across these nations to start the discussion on cross-border interoperability and address fragmentation. The mapping focused on three key areas: comparing core concepts and definitions (finding a "quite good of a matching" and similarities across 10 concepts), aligning levels of assurance (LOA), and mapping international technical standards references.

The mapping results showed that while concepts and definitions aligned well, differences increased at higher levels of assurance, particularly concerning evidence requirements. The report suggests an opportunity for greater collaboration focusing on these higher assurance levels. Furthermore, out of 50 technical standards referenced across authoritative documents, few overlaps were observed across all G7 members, indicating that more work is needed to map and define the relevance of international technical standards to help countries collaborate toward future interoperability.

Overview on State of the Art Wallet Standards

Category: Global I **Speakers:** Paul Bastian (Bundesdruckerei), Daniel Fett (SPRIND) I **Co-organisers:** W3C, OpenWallet Foundation, OpenID, IETF, ETSI, fido, ISO, CSC, GlobalPlatform, MOSIP I **YouTube:** Link

This Panel provided a comprehensive overview of the interconnected standards organisations working on digital identity and wallet ecosystems, establishing a common architectural framework involving three main entities - the issuer, the holder with their wallet, and the verifier or relying party - connected through issuance and presentation protocols, underpinned by cryptography, identifiers, trust frameworks, and governance layers. The panellists detailed contributions from multiple standards organisations: the OpenID Foundation developing core protocols for credential issuance and presentation along with the High Assurance Interoperability Profile; W3C providing the Verifiable Credentials Data Model, decentralised identifiers, and the Digital Credentials API; IETF contributing cryptographic layers and the Selective Disclosure JSON Web Token used in the European eIDAS ecosystem; FIDO Alliance offering authentication protocols for improved user experience; Global Platform focusing on secure hardware elements; ETSI handling European regulatory compliance, trust frameworks, and qualified signatures; the Cloud Signature Consortium addressing remote digital signatures; ISO developing comprehensive frameworks including the mobile driving licence standards and generalised credential building blocks; and MOSIP working on proximity protocols for areas with limited connectivity. The panellists emphasised that whilst multiple standards exist for similar purposes, they complement rather than compete, serving different use cases such as enhanced privacy or specific semantic data requirements, and that successful implementation ultimately depends on trust and alignment across these diverse organisations.

Major Applications and Use Cases

Digital Travel Credentials for crossing borders, passenger facilitation and tourism use cases

Category: Digital Travel I **Panellists:** Ciaran Carolan (ICAO), Youn Kim (IATA), Leire Bilbao (VisitBenidorm), Lisette Looren de Jong (Dutch Government), Siddharth Sharma (DigiYatra India), Maarten Boender (4Sure), Laurent Loup (SICPA), Annet Steenbergen (Circletree) I **Co-organiser**: LSPs **YouTube:** Link

Focusing on digital travel credentials, topics around the implementation of verifiable credentials across borders, jurisdictions, and public-private sectors in travel were addressed: ICAO presented their Digital Travel Credential (DTC), building upon the passport's 60-year success as a globally standardised identity document, whilst expanding their Public Key Directory to enable wider verification including with the private sector. IATA emphasised travellers' desire for a single wallet controlling their data and airlines' need for trusted government-issued credentials, calling for government support in establishing interoperability through their One ID standards. The Dutch government's 2024 pilot at Schiphol Airport demonstrated the DTC's effectiveness, reducing passenger processing from 30 seconds to 10 seconds by enabling advance checks during flight,

leading to a three-year expansion for all EEA citizens travelling outside Schengen. India's Digi Yatra Foundation showcased their operational solution deployed across 24 airports, processing over 60 million verifiable claims with zero personally identifiable information storage, using facial recognition as boarding passes with data deleted within 24 hours. The hospitality sector, represented by Benidorm managing three million annual tourists, highlighted friction from regulatory data collection requirements, whilst ForgeRock and SICPA called for defining a minimal viable interoperability profile bridging regional standards and establishing trust infrastructure for verifying both border authorities and industry relying parties. SICPA demonstrated the ISO PhotoID concept standard, which addresses both border authority requirements and industry data minimisation needs, successfully tested within the EU wallet consortium and requiring governance and country adoption to move forward.

Digital Educational Credentials

Category: Education I **Speakers:** Stefan Liström (SUNET), Klaas Wierenga (GEANT), Kerri Lemoie (DCC) I **Co-organisers:** LSPs, DCC I **YouTube:** Link

Digital credentials in education represent one of the most complex challenges in achieving global interoperability due to education's simultaneously local and universal significance, encompassing formal degrees, upskilling, and informal learning including micro-credentials across a lifetime. The Digital Credential Consortium advocates for open standards such as W3C Verifiable Credentials, which originated with education use cases, and education data models like the European Learning Model and Open Badges 3.0, emphasising that credentials must be trusted, privacy-preserving, and serve human agency rather than surveillance. With international student mobility tripling to nearly 6.9 million between 2000 and 2022, credentials must work seamlessly across borders, requiring extensive vocabularies readable by both humans and machines. GÉANT's eduGAIN federation already handles billions of monthly transactions globally, highlighting the practical challenge of transitioning existing infrastructure to digital wallet systems without disrupting hundreds of millions of users, necessitating parallel operations and flexible governance frameworks including OpenID Federation. European large-scale pilots such as DC4EU have focused on harmonising diploma structures and professional qualifications for digital wallets, whilst upcoming initiatives like WE BUILD and APTITUDE will address the ambiguous concepts of micro-credentials and skills, aiming to integrate public university degrees with private sector learning achievements into portable, lifelong learning records that facilitate both educational progression and employment verification worldwide.

Credentials Beyond Borders - Charting the Future of Health Wallets

Category: Health I **Panellists:** Dr. Alain Labrique (WHO), Dr. Daniel Vreeman (HL7 International), Dr. Osama El Hassan (Dubai Health Authority) I **Co-organiser:** WHO I **YouTube:** Link

The critical challenge of enabling secure cross-border exchange of health data was addressed, as people increasingly travel whilst their medical information remains trapped in disconnected systems. The World Health Organisation's Global Digital Health Certification Network (GDHCN) provides a trust framework, not a data repository, that allows 82 participating countries covering two billion people to issue, verify, and accept digital health credentials bilaterally using cryptographic signatures, built on HL7 FHIR and International Patient Summary standards whilst maintaining sovereign data control. The Hajj Health Card Initiative exemplified this approach's life-saving potential, where Saudi Arabia worked with Oman, Indonesia, and Malaysia to enable over half a million pilgrims to carry verifiable health records, implementing the system in under two and a half months once governance issues around data viewing versus storage were resolved. Additional use cases under development include e-prescriptions for chronic pain patients, maritime health records, healthcare worker credential verification, and disability benefits documentation. However, speakers emphasised that technology

alone is insufficient; success requires enabling policies, clear governance, legal frameworks, and careful attention to equity and financial sustainability to prevent new digital divides, with the fundamental goal of ensuring that a QR code on one's phone could genuinely mean the difference between life and death in emergency situations whilst respecting individual rights and national sovereignty.

Humanitarian credentials and wallets

Category: Humanitarian, Payments, Digital travel I **Panellists:** Juriaan Laas (IFRC), Volker Schimmel (UNHCR), Nelson Goncalves (IOM), Emrys Schoemaker (Caribou Digital) I **Co-organiser**: UNHCR I **YouTube:** Link

The humanitarian sector faces critical challenges in implementing digital credentials and wallets, particularly severe siloing where systems across health, food support, and education sectors remain disconnected despite pressure for interoperability, complicated by organisations' legitimate needs to protect mandate-specific data and competitive advantages in securing funding. A second challenge involves transitioning support from humanitarian organisations to longer-term development actors and social protection systems, requiring technologies enabling smooth, safe handovers. Third, operations occur in contexts with very low digital maturity where people lack connectivity and smartphones, all intensified by an ongoing funding crisis. The IFRC illustrated these issues through a flood victim named Amelia who, lacking identification documents, had to repeatedly re-register at different shelters because systems didn't connect even within the same organisation's network of 191 national societies. IFRC has piloted functional digital IDs and wallets in Kenya and Uganda (2019-2023) through the DIGID Consortium, enabling displaced people to access health services and cash assistance, and developed Access RC, a mobile app for self-registration with automated identification validation. The IOM emphasised that irregular migrants without legal digital identity cannot access services, education, banking, or business opportunities, highlighting that whilst developing countries use digital identity to facilitate trade at land borders, major obstacles persist around recognition, with domestic services often refusing to accept digital credentials and cross-border recognition requiring complex agreements between states and airlines, alongside interoperability issues across databases, legal frameworks forcing people to return to places they fled to obtain documents, and fundamental concerns around data protection and cybersecurity.

Drivers License

Category: Drivers License I **Speakers:** Mike McCaskill (AAMVA), Chris Goh (Austroads), Alan Stapelberg (Google), DB Brudnicki (Apple, Inc.), Florent Tournois (France Titres) I **Co-organisers:** AAMVA, Austroads I **Slides:** Link

This session provided an introduction to mobile driving licences, examining the foundational requirements that initiated their development. The discussion encompasses interoperability and issuer sovereignty considerations, key aspects of the present technical implementation, practical deployment factors and current progress, as well as future directions for this technology.

Digital Car Keys

Category: Car Keys I **Speaker:** Bahar Sadeghi (Car Connectivity Consortium) I **Co-organiser:** Car Connectivity Consortium I **YouTube:** Link

The Car Connectivity Consortium (CCC), a standardisation body with over 300 member companies globally, has developed a digital key solution that enables vehicles to integrate seamlessly with users' digital ecosystems whilst addressing the fragmentation caused by proprietary manufacturer systems.

The CCC Digital Key provides standardised, interoperable access across all phone platforms, vehicle types, and smart devices, with security ensured through storage on tamper-proof secure elements within digital wallets. The solution supports flexible key sharing with customisable privileges, utilises three wireless capability combinations (NFC, Bluetooth Low Energy, and Ultra-Wide Band for hands-free entry), and is already implemented across millions of devices and vehicles with a certification programme ensuring security and interoperability. Looking forward, the CCC is focusing on fleet management applications, where server-based key delegation can significantly reduce operational overhead for rental companies and municipalities, whilst also exploring opportunities to integrate digital keys with other credentials such as mobile driving licences and payment solutions to create comprehensive digital customer journeys.

ID Meets Instant: Enabling Trusted, Inclusive Fast Payments Through Digital Identity

Category: Car Keys I **Speakers:** Guillermo Galicia Rabadan (World Bank), David Black (Digital ID expert) I **Co-organiser:** World Bank Group I **YouTube:** Link

The World Bank's global payments team identified a critical disconnect in the digital public infrastructure landscape: the siloed operation of national digital ID schemes and fast payment systems. Whilst fast payment systems have scaled to over 100 implementations globally, including India's UPI with 700 participants and Brazil's Pix with 900, they continue to face challenges with onboarding, fraud prevention, and account access, issues that could be addressed through better integration with national ID schemes holding valuable but underutilised financial sector information. The team proposed two interconnected solutions: a "Trusted Access and Credentialing Hub" serving as an overlay service to anchor trust frameworks, manage user consent, and orchestrate information flow between systems; and a "Payments Identity Credential" (PIC), a verifiable credential combining national ID and financial sector data to create customer due diligence files, transaction histories, and authentication credentials. Key use cases include remote account opening, fraud prevention through confirmation of payee, improved access to credit via payment data credentials, wallet interoperability across multiple payment service providers, delegation to AI agents for automated transactions, and enhanced user control over personal financial data. The initiative aims to bring these capabilities particularly to developing nations, delivered through digital ID wallets, payment service provider applications, or QR codes, whilst the team actively seeks collaborative input from payments experts, standards bodies, and legal professionals to develop policies, guidance, and standards that can be adapted to different national contexts and maturity levels.

Digital Signatures

Category: Digital signatures I **Panellists:** Viky Manaila (CSC), Arno Fiedler (ETSI), Andrea Valle (Adobe), Chris Tullis & Nay Constantine (WBG), Tolis Apladas (EC) I **Co-organisers:** CSC, World Bank Group, ETSI **YouTube:** Link

This panel discussion on digital signatures examined three critical pillars: global implementation, interoperability standards, and cross-border legal recognition. The World Bank emphasised that digital signatures are fundamental to the entire digital identity ecosystem, as verifiable credentials depend on them for data integrity and trust, whilst warning of the "curse of partial digitalisation" where users can complete simple online transactions but must revert to physical processes for meaningful interactions like obtaining credit or insurance. A risk-based approach was advocated, balancing sophisticated PKI technology's high trust levels against cost and usability considerations, particularly for low and middle-income countries. Adobe presented the Cloud Signature Consortium's success in creating open, vendor-neutral APIs that now connect over 80 members with more than 100 implementations globally, spanning every continent and enabling remote digital signatures

accessible from any device. ETSI confirmed successful interoperability across European and international trust services, whilst developing policies for qualified signatures and attribute attestations through collaborations with OpenID and the CA Browser Forum. The European Commission addressed the primary challenge of legal frameworks rather than technical issues, highlighting their Third Countries Trust List programme for mutual recognition of qualified trust services and plans to trigger Article 14 of the eIDAS Regulation. All panellists agreed that trust is paramount, emphasising that whilst wallets receive attention, the real progress lies in maturing standards, evolving governance frameworks, and technology converging with practice, encouraging countries to adapt these approaches to extend trust across borders.

Trade facilitation in an increasingly complex world - using verifiable supply chain data

Category: Trade I **Panellists:** Nancy Norris (UN/CEFACT), Steve Capell (UN/CEFACT), Sin Yong Loh (Independent Consultant), Alina Nica Gales (Public Corporation of Land and Business Registrars of Spain), Drummond Reed (The First Person Project), Stephan Wolf (Verifiable.Trade Foundation), Brett Hyland (UN/CEFACT) I **Co-organisers:** UNECE, Verifiable.Trade, FIDES, Ayra I **YouTube:** Link

International trade, valued at $25 trillion annually and representing one-quarter of global GDP, faces significant inefficiencies due to its reliance on paper-based processes, with approximately 12 documents accompanying each of the 10 billion consignments moved yearly, consuming roughly 15 million trees. Border and regulatory frictions add $7 trillion in costs, whilst $3 trillion in trade finance requests are rejected due to concerns about document integrity and trader identity. The panel explored how decentralised verifiable credentials can address these challenges by enabling peer-to-peer communication similar to email, avoiding the interoperability problems of platform-based solutions that different countries won't universally adopt. Singapore demonstrated the economic benefits of digitalisation through initiatives like TradeNet and TradeTrust, supporting an economy where trade represents three times GDP. The Spanish Business Registry highlighted how trust technology can embed existing institutional authority into digital systems through their Global Trust Registry project, which builds upon rather than replaces national identifiers. The unique architecture required for trade differs from typical wallet-based identity systems, as documents pass through six or seven handoffs with the consignment itself effectively serving as the holder. Beyond identity verification, product conformity assessment - involving potentially millions of daily certificates - requires digital processes to maintain connections between claims and physical products throughout supply chains. Sustainability regulations are driving development in this space through initiatives like the UN Economic Commission for Europe's certificate exchange work using verifiable credentials.

Framing Organisational Credentials - From Wallets to Impact

Category: Credentials I **Panellists:** Ivan Mortimer (GLEIF), Darrell O'Donnell (AYRA), Vasily Suvorov (Accelerate) I **Co-organisers:** GLEIF, World Bank Group I **YouTube:** Link

Over the past 25-30 years, the digital economy has dramatically reduced transaction costs and enabled global business connectivity, but this growth has inadvertently attracted significant fraud and scams, particularly in faster payment schemes. This has prompted regulators to respond with blunt instruments that have created a bottleneck characterised by both low trust and high friction. The session emphasised that whilst the technology for verifiable credentials is largely sufficient, the critical challenge lies in moving beyond technical cryptographic trust to incorporate human trust through proper governance frameworks that can verify whether issuers are legitimate institutions rather than fraudulent actors. Panellists advocated for a composable, stackable governance approach consisting of three layers: a thin, wide base layer providing broad capabilities like assurance levels and liability models; an industry-specific layer for sectors such as trade, education, and finance; and a

specialised layer respecting jurisdictional sovereignty. The system must handle significant complexity including linking natural persons to legal entities they represent, managing contextual roles that change rapidly, accommodating multiple organisations working across borders, and eventually enabling trust in machines and AI agents, all whilst allowing proper delegation of credentials that can be traced back to authoritative sources. Upcoming session on Day 2 will explore practical applications, how verifiable credentials are used to expand small and medium enterprise access to finance, and strategies for serving the large informal economy where digital companies cannot prove their identity or harness their data effectively.

Digital Assets for DPI

Category: Open source I **Panellists:** Ramesh Narayanan (MOSIP), Anita Mittal (GIZ), Ani Popiashvili (World Bank), Daniela Barbosa (LF Decentralized Trust), Sean Bohan (OpenWallet Foundation) I **Co-organisers:** World Bank Group, MOSIP, LF Decentralized Trust, OpenWallet Foundation I **YouTube:** Link

This panel discussion on digital assets for DPI explored how open source software and open standards serve as foundational enablers for digital public infrastructure globally. Speakers described digital assets operating at two levels: as foundational components including open source software and interoperable standards for payments, identity, and data sharing systems, and as innovative tokenised solutions like bond tokenisation projects and blockchain initiatives for development fund traceability. Challenges were noted around unclear regulatory frameworks, legacy system integration, and cross-border standards. Identity and credential systems were showcased as modular, standards-based solutions with complete credential lifecycles from issuance to verification, currently live in seven countries serving over 130 million people, including rapid deployments of 30 million registrations during COVID-19. The social protection sector's interoperability gap was addressed through system-to-system data exchange frameworks enabling targeted poverty assistance, integrated beneficiary registries across hundreds of programmes, and proactive delivery for populations facing digital literacy challenges. The importance of neutral foundations was emphasised, highlighting that success stems from building communities and providing governance frameworks rather than direct engineering resources, with projects progressing from pilots to production use in various governments and enterprises. Throughout the discussion, speakers stressed that open source's strength lies not only in permissionless innovation and avoiding vendor lock-in but fundamentally in the collaborative diplomacy enabling diverse stakeholders to work together effectively, with open standards creating a level playing field for both public and private sector participation.

AI for Humanity: Uniting Global Forces for an Open, Responsible, and Impactful AI Future

Category: AI I **Speaker:** Annie Lai (Generative AI Commons, LF AI & Data) I **Co-organisers:** OpenWallet Foundation, LF Decentralized Trust I **YouTube:** Link

The challenge of building AI systems that serve all of humanity has become urgent amidst explosive industry growth, from ChatGPT to DeepSeek. Rapid, siloed development by a handful of companies risks leaving populations behind and creating technology fragmentation, making openness essential, indeed using open tooling, models, data, and transparent practices to ensure diverse global perspectives are involved. Day 2 “AI for Humanity track” will feature the following five discussion areas: responsible AI (embedding ethics and governance throughout development, including a collaboratively-defined framework to combat corporate "open washing"), reliability and maturity evaluation (establishing agreed measurements for trustworthy systems), social and economic impact (bringing together experts from psychology, anthropology, and linguistics), and agentic AI

(addressing how to trust billions of autonomous agents acting on our behalf, particularly relevant to digital identity and trust). The core message is an invitation for technologists, policy makers, and advocates to participate in building AI openly, responsibly, and collaboratively, ensuring every voice shapes humanity's AI-enabled future.

Recap Day 2 – Collaborative Sessions

Day 2 of GDC25 was dedicated to collaboration and active participation, guided by the concept of an unConference (Open Space Technology). Although inspired by that concept and other unConferences such as IIW, the organisers decided against calling the sessions on the day itself. Instead, they executed an *"unConference session calling process"* over the preceding weeks (and nights) together with the co-organisers to compile the sessions and schedule in a collaborative effort. The final agenda featured around 100 sessions spread across the day, with up to 15 sessions taking place in parallel.

Attendees were highly encouraged to be active participants and collaborators. Hence, adhering to the unConference spirit, attendees had complete freedom in their participation, noting that participants were trusted to know what would bring them the most value: they could attend the session(s) they wanted, leave a session at any point, choose to end a session or take a break instead of attending a session. This approach granted significant autonomy to attendees, maximising their ability to extract relevant insights and value.

A critical element of such a participatory process is the capture and dissemination of session discussions and outcomes, especially since no one could attend all the sessions. In accordance, GDC25 participants documented the sessions to share learnings with other participants. This documentation has been done under the Chatham House Rule, meaning that the session notes do not attribute specific comments to identifiable individuals. Out of the approximately 100 sessions held during Day 2, participants documented and submitted notes from 26 sessions, following hereafter in alphabetical order. A comprehensive list of all Day 2 sessions can be found in *Annex 2*, also in alphabetical order.

A Smart Health Wallet: Privacy & Control in Your Hands

Category: Global, Health Humanitarian I **Speakers:** Carl Leitner (WHO), Jason Taylor (Google), Alan Stapelberg (Google), Grahame Grieve (HL7), Konstantin Hyppönen (European Commission - CNECT) I **Co-organisers hosting this Session:** European Commission, WHO

Key takeaways:

- The session's goal was to demonstrate a functional Health Wallet prototype, showing the secure carrying, presenting, and verification of digital health proofs using open standards.
- A core focus was the practical application of selective disclosure, a feature highlighted from a policy perspective as integral to protecting sensitive health data and building a trusted health ecosystem.
- Google provided a live demonstration of a wallet prototype, showcasing the end-to-end user journey of adding a health credential (an IPS or ICVP - Vaccine Certificate) to the wallet and presenting it for real-time verification.
- HL7 (Grahame Grieve) provided a technical deep dive on the International Patient Summary (IPS), a globally accepted interchange format for essential health data, built on the HL7 FHIR standard. The demonstration included open-source tools for generating, viewing, and validating IPS documents.
- The discussion identified several key challenges unique to health wallets, including:
    - The large size and complexity of health summaries.
    - The need for users to manage health information for others, such as family members.
    - The healthcare system's general distrust of partial or patient-provided data due to liability concerns.

Next steps:

- Continue developing strategies to ensure health wallets and their privacy features are accessible and usable for all individuals, preventing the creation of a new digital divide in health.
- Further refine the architecture of wallets to handle credentials from multiple authoritative sources and address future challenges like merging health records while maintaining data provenance.
- Promote the use of open-source tooling for creating and validating IPS documents to lower the barrier for adoption by developers and health systems.
- Address the complex policy and technical challenges around consent and the management of health data for dependents within a digital wallet framework

---

Agentic AI and Digital ID

Category: Global, Payments, Digital assets I **Speakers:** Carl Leitner (WHO), Jason Taylor (Google), Alan Stapelberg (Google), Grahame Grieve (HL7), Konstantin Hyppönen (European Commission - CNECT) I **Co-organisers hosting this Session:** Decentralized Identity Foundation, LF Decentralized Trust

Key takeaways:

1. The "Internet of Agents" is Coming

- AI agents will soon interact autonomously across trust boundaries
- Current protocols (like MCP) are driving rapid agent deployment but lack security & trust layers
- We're moving from isolated AI tools to interconnected agent ecosystems

2. Trust Infrastructure is Critical Missing Piece

- 96% of IT professionals recognize AI agents as security risks but are deploying them anyway
- Traditional security frameworks are inadequate for autonomous AI systems

- Current internet security is breaking down under AI-era challenges

3. Identity Management for Agents ≠ Human Identity
- Non-Human Identities (NHIs) have fundamentally different requirements
- Need for dynamic capabilities, lifecycle management, and interoperability at scale
- Both software AND hardware identity components are essential

4. Governance & Liability Gaps Exist
- Agents aren't liable, but their operators are - creating new organizational risk
- Rapid regulatory growth globally (especially Russia, US, EU)
- Need governance frameworks at government, organizational, and individual levels

5. Trust Spanning Protocol (TSP) as Foundation
- Provides authenticity (who said what to whom) and privacy protection
- Designed for interoperability across diverse AI ecosystems
- Ready for advanced AGI capabilities (Levels 3-5)

Next steps:

For Organizations

1. Assess Current AI Agent Deployments
    - Inventory existing AI agents and their data access levels
    - Evaluate security gaps and trust requirements
    - Identify human-in-the-loop requirements
2. Develop Agent Identity Strategy
    - Plan for agent discovery, access controls, and delegation frameworks
    - Establish policies for agent governance and lifecycle management
    - Consider trust/attestation chain requirements
3. Prepare for Compliance
    - Monitor AI regulation developments in your jurisdictions
    - Develop internal governance frameworks for agent deployment
    - Plan for authentic content verification (C2PA implementation)

For Technical Teams

1. Experiment with TMCP (MCP over TSP)
2. Implement Content Authentication and Creator Assertions and communicate that content over TSP

For the Broader Community

1. Join Collaborative Efforts
    - Participate in Trust over IP's AI and Human Trust (AIM) Working Group
    - Engage with Decentralized Identity Foundation
2. Priority Topics for Development
    - Agent Discovery: How agents find and learn about each other
    - Access Controls: Authorization, authentication, delegation mechanisms
    - Human-in-the-Loop: Maintaining human oversight and control
    - Trust Registries: Know-Your-Agent capabilities and verification

Resources: Slides

Bridging Governance and Technical Design: DSNP at the Crossroads of Open Ecosystem

Category: Europe, North America, Digital signatures, Digital assets I **Speakers:** Alberto Leon (Harvard's Applied Social Media Lab), Sarah Nicole (Project Liberty Institute), Wendy Seltzer (DSNP), Wes Biggs (Project Liberty) I **Co-organisers hosting this Session:** Project Liberty Institute, Harvard Applied Social Media Lab

Key takeaways:

- Governance design defines how the decision-making process goes, therefore anticipating the desirable and less desirable outcomes of a system.
- While code plays a role, it alone is not enough to address the risks proactively and embed the values behind a project.
- In a decentralized/complex system, choices at one level affect those elsewhere. Governance is necessary to identify the right paths for decisions at every level, make clearer the interconnections and be responsive to the needs of the whole ecosystem.
- DSNP stands for Decentralized Social Networking Protocol, which is an open protocol for social networking and social media. It is not owned or controlled by any one person or company, allowing anyone to build on it or use it. It allows users to have more control over their data, particularly their social graph and allow interoperability and data portability between the platforms building on it.
- DSNP's progressive decentralization is a good example of the governance approaches and technical design challenges. The DSNP governance international meeting show the relevance of these timely discussions
- Key questions raised the need for liability and enforcement within governance frameworks, contributions back to the open-source ecosystem, how to design for more participatory decision-making from the start, and the responsiveness and sustainability of evolutionary governance framework.

Next steps:

- Join the DSNP Governance Working Group by emailing: dsnpfeedback@projectliberty.io. You have the opportunity to engage with over 30 global experts in governance and technology by giving feedback on the governance framework, the mission and principles and eventually run to be elected in the first DSNP steering committee, launch a working group, etc.

Ressources:

- DSNP Overview
- DSNP Governance Framework
- DSNP Mission & Principles
- The Blockchain Governance Toolkit

Conformance Tests

Category: Global I **Speaker:** Joseph Heenan (Open ID Foundation) I **Co-organiser hosting this Session:** OpenID Foundation

Key takeaways:

OpenID Foundation has a comprehensive set of semi-automated protocol tests that can ensure Wallets, Issuers and Verifiers are correctly implementing the OpenID for Verifiable Credential Issuance (OID4VCI), OpenID for Verifiable Presentations (OID4VP) and the OpenID4VC High Assurance

Interoperability Profile (HAIP) specifications have been implemented correctly and in a secure / interoperable way.

Resources:
Slides used are here: https://docs.google.com/presentation/d/1WKjKIR7LfQmo2sf3QHl-FO-4IeOFOo3j/edit?usp=sharing&ouid=102465972242813123436&rtpof=true&sd=true

Instructions for testing:

- How to run conformance tests for OpenID for Verifiable Presentations
- How to run conformance tests for OpenID for Verifiable Credential Issuance

---

Charting the Course: National Digital Health Wallet Use Cases

Category: Africa, Latin America & Caribbean, Asia & Oceania, Health, Humanitarian I **Speakers:** John Mark Esplana (IFRC), Steven Wanyee, (HELINA Africa), Osama El Hassan (Dubai Health Authority), Erick Kitali (Tanzania Government), Matthew Keks (WHO), Roberta Andraghetti (WHO) I **Co-organisers hosting this Session:** WHI, IFRC

Key takeaways:

- This session explored the multifaceted journey of implementing national digital health wallets, drawing on perspectives from international policy, national implementation, regional collaboration, and humanitarian aid. The central conclusion is that while technology is a critical enabler, sustainable success depends on a strategic blend of non-technical factors. A poll conducted during the session asked participants to identify the single most important "super-multiplier" beyond technology. The top response— "Continuous and Visible Political Championship at ALL Levels of Government, coupled with an aggressive, Public Awareness Campaign" —crystallized the session's core themes: successful digital health ecosystems are built not just on code, but on strong governance, public trust, and inclusive design.
- Other Key Takeaways include:
    - Political Will as the Foundational "Super-Multiplier": The session underscored that sustained political championship is the most critical non-technical driver for success. As demonstrated by Tanzania's progress, strong political will translates vision into mandates, secures necessary resources, and breaks through bureaucratic inertia. This insight was reinforced by the audience poll, which identified this as the top factor for enabling complex initiatives like integrating health wallets with national Digital Public Infrastructure (DPI) and achieving regional interoperability.
    - Public Trust and Inclusive Design are Imperative: The second key theme from the poll was the necessity of public awareness campaigns to build user trust and drive adoption. This directly addresses the challenge of user acceptance and the humanitarian imperative, raised by the IFRC, to design inclusive solutions that empower, rather than create barriers for, vulnerable populations who may have lower digital literacy or lack formal identification.
    - A Solid Regulatory and Technical Framework is Essential: Progress is contingent on a clear policy landscape and robust technical architecture. The 2024 amendments to the WHO's International Health Regulations (IHR) provide a global mandate for accepting digital health documents, including vaccination certificates, starting in late 2025. This regulatory push, combined with foundational infrastructure Kenya's "Digital Health Superhighway," creates the structured environment needed for wallets to function securely and effectively.
    - Persistent Challenges Must Be Actively Managed: Despite clear progress, significant hurdles remain. These include practical infrastructure gaps like inconsistent power and

internet connectivity in rural areas, the technical complexity of integrating with diverse legacy systems, and securing sustainable long-term funding models.

Next steps:

- Finalize International Guidance and Standards: The WHO, in consultation with States Parties, will develop and update technical guidance and standards for the issuance and verification of both digital and non-digital health documents. This will help create a harmonized global approach.
- Prioritize Foundational Integrations: Efforts will focus on ensuring digital wallets are aligned with and integrated into the broader national Digital Public Infrastructure (DPI) strategy. This includes leveraging and connecting with national data exchange platforms and digital identity systems for authentication.
- Fostering Political Will and Establishing Clear Governance: A primary recommendation is to focus on securing sustained political championship at all levels of government. This involves translating high-level support into clear national policies and governance frameworks that empower digital health initiatives with the mandates and resources needed for long-term success.
- Focusing on a People-First Approach to Build Trust and Ensure Inclusion: It is recommended to merge the goals of building trust and inclusive design. This means moving beyond one-way public awareness campaigns to actively co-designing solutions with the communities they serve, especially vulnerable populations. This "people-first" approach ensures the technology is user-centric and accessible, which is fundamental for driving adoption and building public trust from the ground up.

Deep Dive session on Digital Travel Credentials: Policy focus

Category: Latin America & Caribbean, eGovernment, Digital signatures I **Speakers:** Annet Steenbergen (EWC/Circletree), Ciran Carolan (ICAO), Gabriel Marquie (IATA), Laurent Loup (EWC/SICPA), Leire Bilbao (Visit Benidorm), Lisette Looren De Jong (NL Government – Ministry Justice & Security), Florent Tournois (Aptitude) I **Co-organisers hosting this Session:** LSPs, OpenWallet Foundation

Key take-aways:

a. Presentations:

1. ICAO presentation on policy structure (international agreed technical specifications; established trust framework; true global acceptance). The speaker also pointed ICAO role as an international stakeholder in securing this mechanism and even at the technical level (matching the virtual and physical component to the electronic passport/ICAO DTC). ICAO main challenges are trying to extend the ecosystem, exchanging public keys and supporting possibilities for the public and private sector.
2. Netherland representative presentation on DTC-1 pilot led in Schiphol Airport. Key findings: data minimization was a focus and turned out to be a challenge to keep contact with the passengers. Nevertheless, the pilot showed biometric boarding and border crossing treatment significantly faster. New pilot announced for next year: 2-3 years with 1 000 of passengers per day and several airports connected to Schiphol airport. Long term storage and secure wallet around DTC will ensure multiple trips. Finally: control time reduced from 30 sec to 10 sec compared to SSPC (Self Service Passport Control) eGate.
3. IATA presentation, the speaker pointed a couple of issues to tackle with DTC pilots: problems happen when booking information do not match with check-in information; DTC does not support selective disclosure so far which goes against data privacy.
4. Visit Benidorm presentation of PhotoID pilot led in Benidorm area (Spain). The purpose of the experimentation was enhancing hotel check-in (online and at the desk) using the EUDI wallet to

facilitate the user-experience and data collection for the relying parties (hotels). A Spanish citizen was the first European to test in Benidorm the digital wallet that will replace the DNI, health card, visa for work and even plane tickets

5. Aptitude presentation with a focus on DTC use cases: Border crossing, Tickets & check-in. The pilot will be around border control, using DTC Type 2 to reduce congestion and waiting time at the airports, it will also reduce identity fraud and facilitate onboarding and finally reuse DTC data for related transactions – relying on ICAO specifications.

b. Debate:

What would it take from a policy perspective to find an agreement on uniform standard to use?

1. The Dutch governance model is very interesting to find something that suits everyone. Backwards compatibility process is mandatory for both DTC and electronic passport.
Recommended practices to leverage such a digital passport. Business process will be interested to obtain such an information.
2. Other speaker: ongoing discussion with Canada to send them the Dutch issued signed attribute depending on what information is required with authenticity
Other speaker: technicity is not an unsolvable problem, same for Design/UX or Interoperability
3. Governance is to be defined if possible with IATA / ICAO endorsing related recommendations to reach this level of security
4. Other speaker: we need to build a proposition with a cross-border large-scale pilot (several are coming, perfect opportunity)

Can we have multiple standards? And if we digitize the passport or info from it, do we need more trust?

1. We need to align on the multiple credentials and related technical standards with care while aligning the Design/UX - same for how the passport chip is made
2. Other speaker: the wallet can endorse multiple, 2 or 3 it is possible
3. Other speaker: yes, on the technical perspective but it needs to be in accordance with Design/UX. Non-EU countries will have other standards anyway
4. Other speaker: UX needs some form of cross-country standard to ensure trust

Any update on DTC type 2 technical specification release? How announced pilots will affect non-EU citizens and how far will biometric be used beyond border crossing (i.e. luggage tracking)?

1. ICAO: the process is ongoing, and definition might involve ISO. However, no perspective yet on DTC type 2 specifications completion and release dates any soon.
2. Other speaker: we focus on EU citizens so far; In Europe, biometrics use (fingerprint in the passport chip) is not authorized except for use at border crossings.

Next steps:

As a follow up of GDC25, there will be a serie of online meetings to explore the opportunity to solve this important issue at a global scale. PhotoID credential (ISO) is a good candidate and might re-use ICAO trust-framework if passport issuing authorities are allowed to sign and issue them in digital wallets. The objective of those meetings is to align on the perspective and sense if there is sufficient political willingness to move forward.

Deep Dive session on Digital Travel Credentials: Technology focus

Category: Global, Digital Travel I **Speakers:** Annet Steenbergen (EWC/Circletree), Laurent Loup (EWC/SICPA), Maarten Boender (4Sure), Ciaran Carolan (ICAO), Anthony Carmoy (Aptitude), Siddharth Sharma (Digi Yatra), Gabriel Marquié (IATA), Ramesh Narayanan (MOSIP), Arjan Geluck (ISO) I **Co-organisers hosting this Session:** LSPs, OpenWallet Foundation

Key take-aways:

a. Presentations:

1. SICPA presentation on Passport attributes global impact on regulated markets (border authorities, payments, hospitality, and travel). The physical passport is an enabler for global interoperability from holder to verifier. However, the digitalization of society requires a digital credential based on a data minimization mechanism, globally accepted trust framework and aligned standards for interoperability. Protocols, Trust anchors and formats are to be specified with associated open standards. The approach for EWC EU large scale pilot is based on PhotoID (ISO): data groups within the chip help building the digital travel credential (DTC) for border management (pre-travel, e-gates, etc.) and single attributes are available individually for the industry regulatory compliance (data minimization and selective disclosure)
2. 4Sure presentation on Global Trust Framework. We need a common and minimum interoperability profile between DTC requirements and potential standards or solution
3. ICAO presentation on "re-use to innovate". Logical data structure (i.e. DG 1 & 2) with digital signature (i.e. DG 15) helps building the DTC but still requires additional security elements for pilots (booklet remains as DTC Physical component)
4. Aptitude presentation (see associated slides) on DTC use cases for border crossing, Tickets & check-in. One solution to explore is to Issue the photo ID as an equivalent of DTC
5. DIGI YATRA presentation on how to make air travelling seamless, hassle-free, and Health-Risk free experience for passengers from entry to boarding gates. The existing solution insists on data privacy with "dKYC" (don't Know Your Customer) : all personal information is purged daily after the flight.
6. IATA presentation on DTC requirements for seamless travel. The speaker believes the DTC Type 1 virtual component needs to be combined with selective disclosure of DG 1 and DG 2, initial implementation of SD-JWT and ongoing exploration using mDOC. More credentials are needed for seamless travel: visa, digital travel authorization, live biometric and boarding pass
7. MOSIP presentation on "Claim 169: bring trusted mechanism across the world". Claim 169 is a compact binary format for representing verifiable credentials supporting biometric binding to the user for offline verification and suitable for QR code-based presentations.
8. ISO/EIC presentation on communication protocols, security protocols, Data model for PhotoID (1 doctype + 3 name spaces) and data preparation for selective disclosure

b. Debate:

<u>How to achieve convergence of standards and how to achieve global interoperability?</u>

1. Convergence of standard requires also convergence of presentation (Design/UX). ISO for example has organized interoperability test events where organizations and states can test both standards and UX amongst each other. PhotoID has been tested successfully by many international wallet providers in Utrecht (NL) in February 2025.
2. Other speaker: a minimal group of data set on paper, online and in proximity will increase the complexity without single standard
3. Other speaker: now we have multiple solutions: some are live others are days away from production. Any change in the value chain will impact the airport but will not disturb it as long as we agree to the data model

Question from the crowddigital identity and passport are not created equal. Not all e-gates accept all digital identity. Should we not rather start from the end user need?
1. Other speaker: from the standard, in the request we can include a list of specific identifiers (root CL). If not on the list, cannot communicate.
2. Other speaker: we need an architecture where the relying party is being recognized across Europe; some government trust is needed across states.

PID in Europe (personal data with number of attributes – photo is optional) versus photoID (personal data with photo)?
1. PID has no unique identifier nor ID picture which does not allow the industry to comply to national, regional or market specific regulations.
2. Other speaker: Photo ID can be used for regulatory purposes for specific industries.
3. Other speaker: in France there will be no linkability

Next steps:
An alignment on policies is necessary to drive the technical discussions. Indeed, different technical options are available to solve this issue globally. However, protocols decisions will largely reflect policies alignments and objectives. Therefore, meetings on technical standards will follow meetings on policies.

Education Credentials and Digital Human Rights

Category: Global, Education, eGovernment I **Speakers:** Open Discussion led by Kerri Lemoie (DCC), Kim Hamilton Duffy (DIF) I **Co-organiser hosting this Session:** Ayra, DCC, DIF

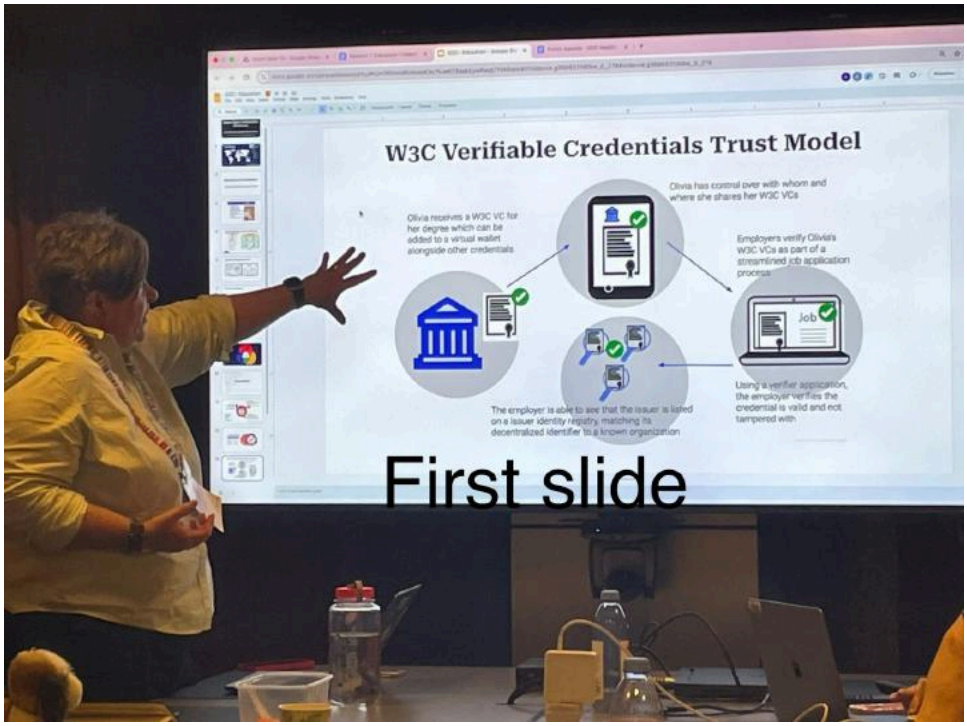
Attendees:
- Kerri Lemoie - Director, DCC, advance use of W3C VCs in higher ed, Director of the Digital Credentials Consortium DCC. We are helping make VC recognized in the education sector in 16 higher educational institutions, Expert in the web tech, specializing in decentralized technologies and standards such as VC and DiD, Founding technical contributor to the Open Badges initiative. She has held exec roles e.g., CTO of Archivery and CEO/CTO of Open Works Groups
- Gillian Walsh - Operations and Project Manager, DCC, communication & education about VCs
- Etan Bernstein- Velocity network, HR technology services and systems, edtech and background screening etc., specialized in HR services, HR systems, backgrounds systems companies, trust framework, services in the education world
- Joe Andrieu - Legendary requirements, LER wrapper, involved in DID WG and W3C VC working group
- Jan Popovic - connect hospitality ecosystem together, capture skills interoperably
- Fatima - GIGA, UNICEF and ITU, student (target audience) in international relations
- Karolina - ITU looking at connectivity and digital transformation in education
- Ildiko Mazar - ELM, get standards to be interoperable, learner centered, etc. co-chair of W3C VC-EDU, NTTData European Commission initiative representative. They want to become interoperable with each other no matter which technology supports career development. VC for education passports.
- Anthea - authority in Singapore, looking at VCs are worthwhile as a utility in singapore, have OpenCerts which is the blockchain verison in singapore
- Princilla - looking towards updating standards to support VC standard
- Wesley Teter - UNESCO higher education and academic freedom

- Phil Long - US Chamber of Commerce and T3 Innovation, advanced skills based hiring and advancement and TLN
- Rupert Ward - Prof Learning and Innovation, work in personalized learning and skills
- Rachel Scherer - gates foundation, works in data systems that promote higher education
- Gabriela Sarmiento - Founder and VP Save My Identity, NPO in Zurich and co-founder Blockchain for Human Rights with Apatride Network, Coalition for Venezuelan and The Rohingya Project. Mentioned best practice where NGO is the platform for a job-day between migrants, refugees and employers. (Manos Veneguayas).
- Rob Schwartz - worked with DCC on year to work on Issuer Identity Registry, worked at Linux Foundation Public Health
- Esther - “Generic smartass” in digital identity, testing and interoperability, “the plunger at the drain.”
- Stefan Listrom - SUNET, swedish research and education network, trusted identity background, large scale pilots in EU, interested in understanding perspectives in this ecosystem
- Jan Meuhlig - ICoBC, interested in experience layer, learning achievement as celebration (using, not just storing)
- Lluis Arino - public university in Spain, convening for education at EBSI (european Blockchain services infrastructure) DC4EU (align EBSI and eiDAS)
- Simone Ravaioli - recognition is a human right, this is the principle of VCs, works in Instructure, co-charing VC-EDU, stewarding OBv3, Credential Engine
- Shigeya Suzuki - Professor at Keio University, information systems architecture, use case focus education credentials, design how they can be used domestically
- Arabella - Learning Economy Foundation, strategy and implementation for scaling adoption of VCs, AI LMS called future frequency
- Kim Hamilton Duffy - Executive Director DIF, Blockcerts, enable standards that allow people to control their credentials and express wide range of skills needed in education, large focus on meaningful consent in SSI (self-sovereign identity), standards in their design have consequences, blog series (will link)
- Sharon Leu - Removing barriers people face in prospering, technology can be a stumbling block, support the development of open standards, Jobs to the future. She removes barriers that people have to endure when trying to find a job. Technological barriers and others. try THAT credentials are recognized and interoperable. She worked on the US depart of education and labor. She used to administrate admin registries. The integrity and security and privacy of the databases have been neglected on purpose but also unintentionally. Now some of these databases have now been used for other purposes during the current US mandate. There are more databases now involved. There is no immediate correlation.

Notes:

- Background/drama: Conversation at IIW led to examination of mDL spec. implementation favored server retrieval (“phone home”) because it's more “technically official.”
- What is the use case that justifies server retrieval?
    - Easy to implement with OpenID server and a user requested the feature.
    - Only obvious use case is surveillance. “Better to have interoperable surveillance.”
    - If it is taken out of the standard, it could still be done.
    - VC API may have a similar problem
- Integrity of US databases has been compromised, intentionally and due to neglect. So now, some of them are correlatable. Education data plays into background checks etc. Who touches your data? What rights do we have?
- Can add payable functions to these trackable and traceable elements

- We can choose to not include the functionality in the standard
- If this is inevitable, we can at least let people know. Not everyone will have a choice.
- GDPR - anywhere that has GDPR then wouldn't be able to implement (or they would be fined for doing it)
- "Phone Home" in the education world. Customers want to know which of the credentials are being used and how often and where. They are selling this as a feature.
- Policymakers - "What is a quality credential?" The answer depends on what is being used and consumed. Therefore, the above data is useful to policymakers. And they want to know if they are asking for the right ones.
- There are a lot of research questions in this space. But the problem is they are not scaling the consent.
- Is there a technical work item that can guarantee anonymity of data? Analyse data in selected student enclaves. (this project may not exist anymore).
- VCDM use cases states - it wants to let the issuer remain authoritative for credential status (but without phone home).
- Socialize the idea that revocation should not be public. (e.g. if you have your ID checked at a bar the bartender doesn't need to know your drivers license has been revoked)
    - Unless it's already been revoked?
- Policy should be monitorable.
- Digital identity - revoke the biometric passport. (eg. If Venezuela revoked a hard copy passport, no one would notice in the Schengen area. But they would if it were digital.)
- First responder - they want to know/track. There may be a range where informed consent is reasonable.
- Giving consent - like the cookies on the website. Whenever there is a phoning home you will need to give consent.
- Where is your education data? Who touches it? What rights do you have? We have to ask these questions.
- Introduction to the W3C VC Trust Model:



- In open badges there can be a phone home. Privacy issue.
- Concern: If there are any policies, they most often prohibit server retrieval, but it can be done anyways, although it is prohibited. DCAPI has a similar problem. To what extent should technology be politically agnostic?
- Discussion: Everybody except for the Scandinavians is worried about their governments.
- We should include standards that would tell how to see and use data. But anyone can drop the standards
- Their customers want to know which of the credentials are being used, how often, where, etc., in the credential platforms in the educational sector, because they in good faith want to learn from the usability of the VCs. This is why a lot of platforms use the behaviors of the VC users.
- What is a quality credential? Is it used by industry? Is it used by employers?
- Is there a sign of trust on that VC? For that there is a need to know about its use. So, users do not know that their behavior is being tracked and used for improvements in the platform, e.g. How do we scale the consent of the users? Maybe people might agree, if they were asked. If there were a more privacy driven way to protect the users, they could then consent on the use of their VCs
- UNICEF financed a project to analyze student data. But they believe it does not exist anymore
- It really was not a privacy issue, it was identity deplatform. What comes back from the issuers in real time, we were talking about something of a more important stake.
- Revocation sections should not be public. Only officers of the court or officers of law should know about revocation. But there are many cases where revocation is public. Public Registries should be public.
- It is not mandatory to use the driving license. But if you have the digital driving license they will know about the revocation.
- Company VCs know when and how I behave as an employee.
- This is education credentials. We should approach this problem as a very big deal. This is a community led standards consensus process.
- We need to keep talking about it. It's the only way to create awareness.

Nest steps:

- Establish a working group? Email to klemoie@mit.edu
- Schedule a few sessions at VC-EDU

Resources:

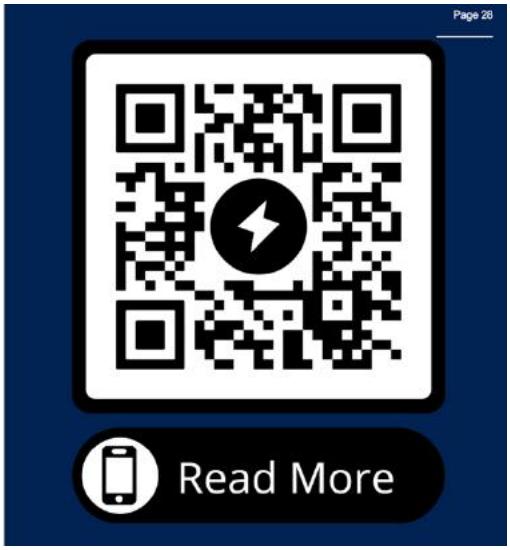
- Original SSI Principles: https://www.lifewithalacrity.com/article/ssi-bankruptcy/
- GDC- Education - slides (including VCDM explanation)
- Notes doc from previous meetings: Public Agenda - GDC Meeting Education Track
- ITU - Building the case for a digital public infrastructure for education (QR code): https://www.itu.int/hub/publication/s-wp-dpi-education-2025/
- W3C VC-EDU Task Force: https://w3c-ccg.github.io/vc-ed/
- No Phone home: https://nophonehome.com/
- Blog series
  - Part 1: https://kimdhamilton.com/latent_surveillance/
  - Part 2: https://kimdhamilton.com/server_retrieval/
  - Part 3: https://kimdhamilton.com/american_privacy/
- Post: The end of the dream for privacy by design and self-sovereign identity wallet due to re-centralisation attempts

GlobalPlatform Technologies for wallets

Speakers: Gil Bernabeu (GlobalPlatform), Mike Bergmann (BSI), Victor Hsieh (Google I **Co-organiser hosting this Session:** GlobalPlatform

Key takeaways:

- Over 70+ billion GlobalPlatform certified SEs; 1 billion TEE
- EUDI Wallet enablers
    - SAM and CSP
- SAM - offers a secure and standardized environment for member states to manage end-user authentication, end-to-end security, and secure storage.



- CSP - solution for composite certification
    - Optimized Secure Evaluation for applet using CSP enabled certified SE
- Android solutions for EU-DI
    - Strongbox solution based on certified eSE and CSP

Next steps:

- Learn more about SE for EUDI

Identity Foundations for Business Ecosystem Transformation and Industry 4.0

Category: Global, Payments, Digital assets, Organizational credentials I **Speakers:** Dr. Juan Caballero (DIF), Dr. Susanne Guth-Orlowski (4TheRecord), Michal Jarmolkowicz (Swiss Safe), André Röder (Kaprion), Steffen Schwalm (msg GmbH), Dr. Carsten Stöcker (Spherity GmbH) I **Co-organisers hosting this Session:** DIF, OpenWallet Foundation

Key takeaways:

The Trust Gap Challenge:

- Critical Problem: While IoT devices can do zero-touch onboarding, most device identities rely on private PKI systems, creating "PKI islands" and visibility gaps
- Solution Direction: Decentralized identity approach using DIDs, VCs, and DIDComm where devices have self-sovereign identities anchored in secure elements

Evolution Beyond QR Codes

- Current wallets are limited to simple QR code interactions
- Future Vision: Intelligent wallet agents with DIDComm v2 enabling:
    - Direct wallet-to-wallet communication
    - Multi-party, multi-step workflows
    - Autonomous decision-making capabilities
    - 33% efficiency gains with CBOR optimization

European Digital Identity Infrastructure

- European Business Wallet (EUBW) launching Q4 2025 as cornerstone of EU digital strategy
- eIDAS 2.0 introduces new trust services:
    - Qualified Electronic Attestation of Attributes (QEAA)
    - Electronic Ledger services
    - Standardized DIDs
- EBSI provides sovereign, pan-European blockchain infrastructure with governmental trust anchors

Industry 4.0 Applications

- Digital Product Passports (DPPs) becoming mandatory for EU Battery Regulation (Feb 2027) and other sectors
- United Nations Transparency Protocol (UNTP) implementing global standards for trusted supply chain data exchange and transparency
- Supply Chain Traceability: Combination of identity and transaction data through qualified ledgers

Healthcare IoT Revolution

- Plug & Play Clinical IoT: DIDComm enables reduction from 5 manual steps to 2 automated steps
- Devices can request passports, auto-onboard, receive credentials, and send provenance data over DIDComm
- Demo planned for DICE conference (Zurich, autumn 2025)

Next steps:

Collaboration Opportunities:

- Contact TRACE4EU consortium for supply chain traceability pilots
- Engage with Global Battery Alliance for battery passport operational trials
- Participate in clinical IoT demo at DICE conference
- Join industry standards development:

    - CEN/CENELEC JTC19 (Harmonised Standards for Decentralised Identifiers)
    - CEN/CENELEC JTC24 (Digital Product Passport System & Framework)
    - DIF (DIDComm)
- DIF to explore development of DIDComm message profiles; contact DIF at contact@identity.foundation if you're interested

Key Contacts for Follow-up:

- DIF: contact@identity.foundation
- SwissSafe/Clinical IoT: michal@swisssafe.com
- Spherity/Industry 4.0: Carsten.Stoecker@spherity.com
- 4TheRecord/UNTP: just@4therecord.io
- Kaprion/Enterprise Security: andre.roeder@kaprion.de
- TRACE4EU: https://trace4eu.eu/

Resources: Slides: Foundations for Business Ecosystem Transformation.pptx

---

Identity Systems and Threats: A Holistic View

Category: Global I **Speakers:** Carolin Beer (ETH Zurich), Sheila Zingg (ETH Zurich), Patrick Schaller (ETH Zurich), Xenia Hofmeier (ETH Zurich) I **Co-organisers hosting this Session:** W3C, OpenID

Key Takeaways:

- Evolution of identity systems from silos, through federated systems, to SSI
- With the evolution of these systems, responsibility has shifted to the holder of an identity (consensus of the user is required for the use of identity attributes)
- Achieving holistic security for an identity system is crucial. Vulnerabilities can have a big impact and user trust may be irreparably damaged.
- Threats are influenced by the desired use cases and the corresponding security properties.
- The threat stack was perceived as useful to identify threats across different components in an identity system, and to assess and visualize the corresponding security guarantees.
- Also the threat stack might help to understand the limitations of security proofs, which typically are associated with a certain layer of the stack (e.g., security protocols) and are valid only in a defined attacker model.
- Last but not least the threat stack may help to assign a given threat with a corresponding layer, allowing to better understand the impact of vulnerabilities.
- Security proofs for components of an identity system may lose their validity if components are combined with other components (may be the case on the same layer or across layers).
- Defining clear semantics for the threat stack while maintaining an appropriate level of abstraction is challenging.
    - Opinions on the position of actors like the regulatory body and the user differed: they could be either represented as part of the threat stack or as external impact that it external to the system boundaries
- Threats are not only defined by the initial design of an identity system but may be introduced by future changes.
- The current usability and interoperability layer contains a variety of threat categories, it may be helpful to specify them more precisely.

Next Steps:

- Incorporate the existing feedback into the threat stack
- Potentially instantiate the system with a specific architecture

Resources: Slides (PPTXs: https://polybox.ethz.ch/index.php/s/6Ns4nYtoSbncGfD)

International Trade: Identity across borders - combining SSI and authoritative registers

Category: Trade, Organizational credentials, eGovernment I **Speakers:** Steve Capell (UN/CEFAT), Alina Nica Gales (registaroes.org), Drummond Reed (Ayra), Jose Cantera (IOTA Foundation), Jeanne Huang (UN/CEFACT) I **Co-organisers hosting this Session:** UNECE, Ayra, IOTA Foundation

Presentations:

- Alina Nica Gales (registaroes.org): The Spanish business register and the UN/CEFACT Global Trust Register project
- Drummond Reed (Ayra network): The Ayra project and how that approach complements institutional identity registers.
- Jose Cantera (IOTA Foundation): IOTA and EBSI and where DLT fits into this picture
- Jeanne Huang (UN/CEFACT): Legal alignment on identity across border and how UN/CITRAL model law on cross border identity may help

Key takeaways:

- High-integrity digital identity is a foundational capability for international trade, enabling customs authorities to reduce illicit trade, financial institutions to expand access to trade finance, and stakeholders to verify sustainability claims in supply chains.
- The UN/CEFACT Global Trust Registry (GTR) project aims to establish a governance framework to recognize authoritative registries (such as national business or trademark registers) as verifiable sources of legal entity identity. The goal is to link these authoritative identities to decentralized identifiers (DIDs) through cryptographically verifiable credentials.
- Self-sovereign identities (SSI) such as W3C DIDs and authoritative identities maintained by sovereign registries are complementary, not competitive. Their combination enhances institutional trust and digital scalability.
- IOTA is developing open-source, DLT-based infrastructure to support interoperability between registries and decentralized identity ecosystems. Their work with EBSI and DIDs enables the issuance and verification of verifiable credentials (VCs) anchored in authoritative registries.
- A key technical challenge is that many registries are not yet equipped to issue or sign verifiable credentials. The GTR project aims to address this by building institutional capacity and technical readiness.
- From a legal perspective, the UNCITRAL Model Law on Identity and Trust Services provides a basis for harmonizing digital identity governance across borders. Key barriers include the absence of enabling national laws, reliance on paper-based identification, and lack of mutual recognition mechanisms.
- The diversity of national registry landscapes (e.g., 176 business registries in Germany) illustrates the need for interoperable frameworks that allow decentralized and authoritative identity systems to work together.
- The vision is not to replace existing systems, but to upgrade them into trust registries that can support digitally verifiable, cross-border identity assurance.

Next steps:

- Support the development and piloting of the GTR framework under UN/CEFACT, with engagement from national registries and identity system developers.
- Encourage more national authorities to explore the issuance of verifiable credentials and participate in open development processes.
- Explore technical integration opportunities with DLT infrastructures (e.g., IOTA, EBSI) to enable decentralized verifiability.
- Promote broader dialogue and adoption of the UNCITRAL Model Law, especially in regions lacking digital identity legislation or recognition frameworks.

Resources:

- UN/CEFACT GLobal Trust Register - Project Overview - https://uncefact.unece.org/display/uncefactpublic/Global+Trust+Registry
- W3C Decentralized Identifiers (DIDs) Specification
- IOTA and EBSI
- UNCITRAL Model Law on Identity and Trust Services
- Registradores de España (Spanish Business Register)

International Trade: Improving Compliance and Facilitation with Verifiable Credentials

Category: Global, Trade I **Speakers:** Steve Capell (UN/CEFACT), Sin Yong Loh (UN/CEFACT), Stephan Wolf (Verifiable.trade), Emily Benett (UNICC) I **Co-organisers hosting this Session:** UNECE, Verifiable.Trade, UNICC

Presentations:

- Steve Capell (UN/CEFACT): The future of trade finance and customs compliance with verifiable trade documents
- Sin Yong Loh (UN/CEFACT): Verifiable /transferrable trade documents - The UN/CEFACT VC4trade project
- Stephan Wolf (Verifiable.trade): Verifiable.trade overview and implementer of VC4trade specifications.
- Emily Bennett (UNICC): The UNICC and examples of trade facilitation and digitalisation

Key takeaways:

- Global trade is still largely paper-based, with trust remaining the main barrier to digitization. Paper processes lead to inefficiencies and vulnerability to illicit trade, including $0.6T in counterfeits, $0.6T in tariff evasion, and $0.6T in smuggling.
- The cost of trade is immense: $2T in tariffs, $6T in transport, and $6T in regulatory frictions, highlighting the need for streamlined, digital processes.
- The trade finance gap remains significant: $3T in unmet demand, with ESG-related compliance adding further costs ($6T+ across biodiversity, due diligence, and emissions).
- Traditional “single window” systems are complex, expensive, and hard to interconnect, limiting their effectiveness across borders.
- Verifiable Credentials (VCs) offer a paradigm shift by enabling trusted, portable trade documents without requiring centralised infrastructure or shared platforms.
- VCs support interoperability and decentralised trust, facilitating both legitimate trade and compliance while curbing illicit flows.
- The UN/CEFACT VC4Trade project provides common specifications to make verifiable trade documents scalable and actionable across customs, finance, and regulatory bodies.

Next steps:

- Support and scale the UN/CEFACT VC4Trade project, including implementation by trade authorities, customs, financial institutions, and industry associations.
- Promote cross-border adoption of verifiable trade documents as a complement or alternative to traditional single window systems.
- Foster collaboration between governments, private sector actors, and standards bodies to ensure interoperability, not uniformity.
- Encourage pilot projects and capacity-building around verifiable credentials for key trade documents (e.g. invoices, certificates of origin, bills of lading).
- Leverage platforms like verifiable.trade and partners such as UNICC to demonstrate real-world use cases and reduce entry barriers.

Resources:

- UNECE VC4Trade Project overview - https://uncefact.unece.org/display/uncefactpublic/Verifiable+Credentials+for+Trade

International Trade: Traceability and Transparency for the sustainable transition

Category: Global, Trade, eGovernment I **Speakers:** Pieter Van der Honing (GlobalPlatform), Chris Goh (Austroads), Joseph Heenan (OpenID foundation), Mike McCaskill (AAMVA), Steve Pannifer (FIME) I **Co-organiser hosting this Session:** GlobalPlatform

Presentations:

- Zach Zeus (UN/CEFACT): UNECE Recommendation 49 and The United Nations Transparency Protocol.
- Susanne Guth-Orlowski (GBA): The Global Battery Alliance as an example UNTP extension owner.
- Beatrice Fernandez (UNEP): UNEP program on digital product information system and lifecycle analysis
- Brett Hyland (UN/CEFACT): Digital Product Conformity (both traditional CASCO style and the Wild West of ESG schemes) - DCC and SVC?

Key takeaways:

- UN/CEFACT Recommendation 49 enables large-scale, trusted sustainability claims in supply chains.
- Sustainability information helps differentiate products but creates risks of false claims.
- Verifiable, high-quality claims allow fair competition on sustainability.
- Target: 1 million Digital Product Passports (DPPs) issued per day by 2030.
- DPPs track sustainability and traceability data at every stage of the product lifecycle.
- Data can be shared, redacted, and updated while protecting sensitive information.
- Business and facility identities are linked to trusted authorities for accountability.
- Conformity assessment bodies validate sustainability claims through verifiable credentials.
- A digital “trust graph” connects validated claims across the supply chain.
- UN Transparency Protocol (UNTP) supports implementation of Recommendation 49.
- UNTP provides a digital solution to prevent greenwashing through verifiable claims.
- Regulated (e.g., EU) and voluntary product passports coexist; voluntary schemes face:
- Proprietary standards
- Compatibility issues
- Assessor competency concerns
- Lack of certificate validity visibility
- Global Battery Alliance (GBA) example:
- Battery passports mandatory in EU by Feb 2027 for >2kWh batteries
- Operational trials start Q4 2025
- Focus on data collection, third-party credentials (e.g., sustainable mining), and site-level reports

Next steps:

- Finalize approval and global adoption of Recommendation 49 and UNTP.
- Scale use of verifiable, digital credentials for trusted sustainability claims.
- Address interoperability and compatibility challenges across standards.
- Support industry trials to test and refine traceability tools (e.g., battery sector).
- Align regulatory requirements with commercial incentives for sustainability.
- Engage all supply chain actors in sharing data, credentials, and site reports.
- Promote continuous improvement and transparency across supply chains.

Resources:

- UN/CEFACT UNTP Project: https://uncefact.unece.org/display/uncefactpublic/Transparency+at+scale%3A+digital+solutions+for+trust+-+resilience+and+sustainability
- UNTP Documentation site: https://uncefact.github.io/spec-untp/

Interoperability for Digital Identity Solutions: Ensuring trust through testing

Category: Global, Drivers licence, Digital signatures, Digital travel, Payments, Car keys, eGovernment I **Speakers:** Pieter Van der Honing (GlobalPlatform), Chris Goh (Austroads), Joseph Heenan (OpenID foundation), Mike McCaskill (AAMVA), Steve Pannifer (FIME) I **Co-organiser hosting this Session:** GlobalPlatform

Key takeaways:

- Interoperability starts at the root.
- Current state of the market in terms of regulation:
    - In North America some policies are still being developed.
    - As in the EU testing is also still in the infancy stage where policies are currently being developed.
    - Speed of developments; in scheme level in the perspective of payments, schemes interoperate through orgs like EMVCo. In contrary, ID and wallets does not follow the same as there are layers in the stack like credentials.
- Governance mechanisms:
    - Complexity is the initial challenge.
    - There are a lot of overlaps that needs alignment we can follow the payments in this regard.
    - Fragmentation comes with a cost.
    - AAMVA: look externally to apply and align internally that's why to take part on other groups.
    - Need for independent review of implementations. What we need but needs a level of coordination: Reference implementations, Test tools.

Next steps:

- Call for collaboration.

Protecting the Wallet - How much security is enough?

Category: Global, Car keys, Digital travel, Drivers licence, Payments, eGovernment I **Speakers:** Fabien Deboyser (GlobalPlatform), Felix Bleckmann (BSI), Marie Austenaa (Visa), David Zeuthen (Google), Sasikumar Ganesan (MOSIP), Herbert Leitold (A-SIT) I **Co-organiser hosting this Session:** GlobalPlatform

Key takeaways:

- **Need for high level of Security**
- Beyond Europe
    - Device binding is an aspect to look into that could solve this.
- The ability to use existing infrastructure like in payments the existing payment terminals. The wallets today need to adapt to this.
- Security Certification
    - Certified secure hardware is a demonstration of strong security.
    - The best way to approach the security problem is certification.

    - Harmonized schemes is the long term goal.
        - Mutual recognition of certificates can be applied during the transition period.
- Secure elements for example are certifiable that demonstrates high level of security.
- The CSP will gives level of assurance high.
- User control:
    - The definition is broad, but to be more specific, it relates to the extent of user control over their information and the ability to selectively disclose it.
- Fragmented device ecosystem
    - In the context phones, standards like the CSP could address this problem.
- Cloud wallet implementation
    - Combination of certified secure elements (SAM and CSP) and have addition of cloud based HSMs.
    - Www wallet an example.
    - Cloud based wallet could be essential for interoperability so security should be ensured in this implementation.

Setting the Bar: Health Wallet Standards, Testing & Compliance

Category: Global, Health I **Speakers:** Grahame Grieve (HL7), Hani Eskandar, (ITU), Cyril Seck (African CDC), Chinemerem Eyetan (WHO), José Costa Teixeira (PATH), Carl Leitner (WHO) I **Co-organisers hosting this Session:** ITU, WHO

Key takeaways:
This technical roundtable focused on defining the essential requirements—the "bar"—for creating secure, interoperable, and trustworthy digital health wallets. The discussion was structured around three key pillars:

- **Foundational Standards:** Panellists explored the core technical building blocks for health wallets. This includes the HL7 FHIR resources and profiles that form the bedrock for health data, as well as other critical standards for identity and credentials needed to complete the ecosystem. A key consideration is ensuring these standards are practical and sustainable for implementation within diverse national digital service ecosystems.
- **Testing & Validation:** The discussion covered the need for realistic testing approaches. This includes aligning health wallet testing requirements with the forthcoming WHO-ITU Reference Architecture for Digital Public Infrastructure (DPI) for Health. From a regional perspective, there are practical challenges and opportunities in establishing shared validation tools, like regional testing sandboxes, to support member states. Implementation partners face real-world challenges in applying global testing protocols in countries with varying infrastructure and capacity.
- **Compliance & Trust:** The panel addressed the need to design compliance and trust frameworks that are credible and robust, yet not so burdensome that they stifle innovation, particularly for solutions developed in the Global South.
- **Healthcare-Specific Challenges:** Beyond the core technical components, the group also considered challenges unique to the healthcare domain. The panel agreed that for the digital wallet concept to succeed, future work must specifically address these challenges, such as navigating complex data privacy rules, ensuring equitable access, and building public trust.

Next steps:

- Collaboratively define and document a baseline of definition, and essential technical and governance requirements for a secure, interoperable, and globally relevant health “wallet”.

- Develop practical and meaningful validation processes and conformance tools that can be adapted to diverse country settings with varying levels of infrastructure and capacity.
- Explore the creation of regional support structures, such as testing sandboxes, to assist countries in adopting and verifying compliant health wallet solutions.

Skills-based Economy & First Person Credentials

Category: Global, Education, Humanitarian I **Speakers:** Darrell O'Donnell (Ayra), Etan Bernstein (Velocity Network Foundation), Wesley Teter (UNESCO), Drummond Reed (First Person/Ayra), Sharon Leu (JFF), Stéphanie Winet (IOE), Joan Beets (KennedyFitch), Tanya Troshyna (Affinidi) I **Co-organisers hosting this Session:** Ayra, LF Decentralized Trust

Session Objectives:

- Discuss the requirements for a global digital skills-based economy and understand where we are on the path towards enabling it.
    - Identify which requirements we agree on
    - Identify where there are disagreements
- Agree on next steps to collaborate to address the differences, remove the barriers and advance the adoption of a viable solution.

Problem Statement and Long Term Goal:
We presented three personas representing real-world challenges in the current labor market.

Vanessa Lin

Registered Nurse

Born, educated and began career in the Philippines (first license and first nursing job, multiple certifications and trainings).

Then moved to Dubai to be a nurse (additional license and job history, new certifications).

Then moved to Netherlands to get an advanced degree in a specialized nursing area.

Then moved to the US. Needs to get a license and a job.

Challenges of global mobility in a highly regulated industry.

Iszak Mulama

Cyber-security specialist

Recent graduate in mechanical engineering from university in Kenya.

From age 14 has been hacker and gamer and has amazing software development and cyber-security skills and knowledge.

Has led a team to win a hackathon at the local university.

Wants to apply to a remote job at a global software company or gig opportunities via a global gig platform.

Challenges of skill recognition from informal learning. Challenges of global employers and global gig platforms

Bot1627

IT Specialist

Resume meets all requirements for each job description.

Identity documents, education diplomas and professional certification documents all look perfect.

Run by North Korean company.

Challenges of AI & increased fraud

In preparation for the session, we drafted 10 statements of requirements and provided them to the participants from their feedback.

Heading	Details
Individual at the Center Solution must be centered around the individual	• Individuals must maintain ownership and control on their credentials. • Individuals must have the ability to consolidate their credentials from all issuing bodies into a single wallet of their choice. • Portability - Individuals should not be confined to a specific wallet and should have the freedom to effortlessly transfer their credentials to other wallets that adhere to the same protocols without losing utility. • Individuals must be able to universally share their credentials with any relying party, without any restrictions or limitations. • Individuals must be able to curate and share a broad or limited presentation out of this collection. Solution must support principles of selective disclosure and data minimization. • The individual must be able to self-assert credentials. Self-asserted credentials must be clearly marked as such yet adhere to the same technical standards and schemas as verifiable credentials and be shared as part of a disclosure, together with other credentials, verifiable or self-reported.
Global Solution must be international / global / (Inter-planetary?)	• Solution must enable individuals to claim credentials in any jurisdiction and share credentials in any jurisdiction. • Solution must support global mobility of Individuals. • Solution must support global employers' ability to receive and verify credentials in a consistent method anywhere in the world. • Solution must be applicable to the unique requirements of different industries and local labor markets. • Solution must support multi-language

Encompass all work-related information
Solution must be broad and encompass all work-related data elements
	• Must support the credentialing of any method of skill attainment:
	  • Primary, secondary and post-secondary education
	  • Training
	  • Work experience, internship, apprenticeship
	  • Self-learning
	• Must support the credentialing of any method of skill assessment and recognition:
	  • Assessment
	  • Certification
	  • License
	• Must support credentialing of any information required to meet job requirements in a country, industry or employer
	  • Work experience
	  • Right To Work (RTW)
	  • Occupational Health records

Assurance, trust & verifiability Solution must meet the highest level of assurance, trust & verifiability	• Must be useful in the most highly regulated industries - healthcare, aviation, oil & gas, education • Must define legal liability of issuers on the credentials they issue. • Individual authentication - Must include authentication methods that enable the issuer to obtain and document rigorous proof required to confirm that the individual is genuinely who they claim to be before issuing them credentials. • Source Verification - Must include authentication methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer of a credential is genuinely the entity they claim to be. • Source Authority Verification - Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer has the authority to assert the claims included in the credential.

Heading	Details
	• Data Integrity - Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the information included in the credential genuinely represents the claims made by the issuer. • Revocation Status Verification - Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was not revoked by the issuer. • Person Binding - Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was issued by the issuer to the individual presenting it.

Compliance (Privacy ++)
Solution must be compliant to all relevant local regulations
	• Solution must be compliant with all relevant regulations that govern data and information in the labor market, including, but not limited to:
	  • Privacy regulations (e.g. General Data Protection Regulation - GDPR)
	  • Employment regulations (e.g. California Privacy Rights Act - CPRA)
	  • Education regulations (e.g Family Educational Rights and Privacy Act - FERPA)
	  • Other relevant regulations (e.g. Fair Credit Reporting Act - FCRA)
	• No "Dial Home"

Survivability Solution must ensure that credentials are survivable of issuer existence	• Data / Assertions must be accessible and verifiable even if the Issuing body no longer exists or no longer has the data.
Open Solution must be based on open standards, open-source technologies	• Serve as an open, public good infrastructure • Support technical and data interoperability • Based on open technology standards • Based on open data standards • No vendor lock-in • Open to support a global community of innovation and development
Presentation/multiple credentials Employers / Organizations must be able to receive a presentation (i.e. "resume") and verify all its content immediately and digitally	• A curated selection of credentials (10s, or maybe even 100s) can be shared by the individual to a relying party in a single presentation. • A complete presentation can be verified by the relying party. • Relying party AI-based solutions will interpret presentation, evaluate, model, and predict fit and success in a role.
Issuer revocation and change Issuers must retain some level of control	• Revocation - An Issuer must be able to revoke a credential held by the user. The user must be notified of such revocation. • Change - An Issuer must be able to force update the data on the credential held by the user. The user must be notified of such update. • The issuer must notify the individual on any credential revocation or credential change event.
Notary Solution must support notary/apostille issuing	• Solution must enable accredited notaries to issue credentials to individuals based on clear criteria of primary-source verification.

Key takeaways:

The panellists each shared their personal and professional view on the challenges and a short description of what they view success will look like. All agree there is incredible friction in the labor market today and verifiable, self-sovereign, digital credentials have the potential to reduce this friction for both individuals and organizations.

In general, there was high level agreement on a number of the requirement statements such as

- Individual at the center
- Assurance, trust & verifiability
- Survivability

We dedicated the majority of the conversation on the panel to the requirement around "**Encompass all work-related information**" and the concern that this is too broad. There were multiple comments

about finding the balance between a goal to accelerate adoption and the long term goal of accommodating this requirement.
We also discussed the requirement of supporting "**Issuer revocation and change**" and the concern about limiting this to specific applicable scenarios where it does make sense to allow the issuer to revoke. Also raised was to ensure that the individual has a right to appeal when an issuer revokes a credential.
The panel members and participants raised the need to clearly identify who the different users are for this solution/infrastructure, and make sure that the requirements of each of the user groups is properly addressed.

Next steps:
Our goal is to take the content that was prepared for this session and that of the panel discussion we held at the conference and publish a document which summarizes the requirements we agree on and highlights the requirements that need our continued attention and work.
We invite the entire community to collaborate and contribute to this work!

If you would like to contribute, please reach out or send your feedback to
etan.bernstein@velocitynetwork.foundation

Sovereign by design: Panel

Speakers: Javier Valiño (Eclipse Foundation), Christoph Strnadl (Gaia-X), Rajiv Rajani (iShare), Etan Bernstein (Velocity Network Foundation) I **Co-organisers hosting this Session:** Eclipse Foundation, Ayra

Key takeaways:
The following questions have been asked to panelist during the session. For each question, a summary of the discussion is provided.

What does "Sovereign by design" mean to you?
Sovereign by design means embedding control, trust, and autonomy into digital systems from the start—ensuring individuals own and manage their data and credentials, organizations can enforce data rights through reliable governance, and ecosystems retain the strategic freedom to choose how trust is implemented. It's not about isolation, but about designing for interoperability and flexibility, so participants can operate confidently and independently within interconnected environments.

[AUDIENCE QUESTION] What is the current status of Gaia-X and Catena-X collaboration? Are there plans for convergence?
Disclaimer: The panelist cannot speak on behalf of Catena-X as they are not represented in the panel, but just to provide their view
Collaboration between Gaia-X and Catena-X is in place, with the idea of converging specially at trust framework level
Additional collaboration between these 2 associations and other Dataspace ecosystem actors is also happening in the Eclipse Dataspaces Working Group, where members are producing interoperable dataspace protocols and open source implementations of those, including for instance Tractus-X project, with tight links to Catena-X.
Tractus-X is precisely a good starting point for whoever is willing to investigate and reuse dataspace components and contribute to the new releases with extended functionalities.

What are the foundational elements for interoperable and trustworthy digital ecosystems?

If you could align on one thing today across your ecosystems to unlock scale, what would it be?
Across all contributions, a strong convergence emerges around the layered nature of trust and interoperability. We have discussed four interoperability layers—technical, semantic, organizational, and legal—extending across both intra- and inter-ecosystem dimensions, echoed by Etan adding up to five (+structural). It was also emphasized the importance of governance and data control as core design principles, reinforcing the idea that interoperability is not just about technology but about who defines the rules and how trust is operationalized. All speakers pointed to trust frameworks as the cornerstone of scalable, sovereign collaboration—each developed for different domains, but sharing a vision of automated, rules-based, and verifiable interactions.
The panellists unanimously recognized that achieving scale requires more than aligned technologies—it demands convergence on shared trust principles and governance models. Despite different domain focuses, all speakers aligned on the notion that operational trust—not just theoretical compatibility—is what ultimately enables scalability. What unites these approaches is the call for composable, modular, and extendable trust infrastructure that can bridge diverse domains and geographies.

How do your initiatives contribute to the vision of portable and verifiable digital credentials, and how do you see the role of digital sovereignty in your domain?
The speakers presented complementary approaches pointing out individual control and cross-organizational trust as essential pillars of digital ecosystems. We have discussed digital credentials as a human right or the need for organizations to transact peer-to-peer while exercising data rights. The unifying thread is clear: sovereignty means control over identity and data—whether by individuals or organizations—and portable credentials are the mechanism to achieve it across domains, without sacrificing trust or compliance.

What are the most urgent interoperability gaps between data sharing ecosystems today—and how can we help close them?
Interesting gaps presented such as lack of consistent, state-issued basic digital identity and misaligned data schemas, cultural and governance challenges, urging stakeholders to embrace reuse over reinvention, protocols and standards being often incompatible at the agent or connector level, and lack a common “language” to define trust across ecosystems. The common ground is clear: semantic, organizational, and trust-model misalignments are now the most pressing barriers. The way forward is not to impose uniformity, but to agree on how diverse trust anchors, credential schemas, and governance rules can interoperate through shared semantics and extensible frameworks.

With growing regulation (e.g., EU Data Act, eIDAS2, CRA), what role do your initiatives play in making compliance easier and more future-proof?
While their approaches differ, all speakers recognize that compliance must be automated, adaptable, and ecosystem-aware. Important topics covered: compatibility with eIDAS 2.0 and the EU Data Act, participation in global standards bodies and harmonization answering regulatory needs. Together, these perspectives underline that compliance isn’t static—it’s a living component of infrastructure design, and that collaborative, open governance is the only sustainable path to both sovereignty and regulatory resilience.

Next steps:
The collaboration towards interoperable standards for dataspaces will continue in the Eclipse Dataspaces Working Group. The audience is invited to follow up and collaborate with the different initiatives there. This collaboration can happen at developer level (on open source project) and also strategical level, joining the working group.
Resources:

- https://dataspace.eclipse.org/
    - Eclipse Dataspace Protocol
    - Eclipse Dataspace Decentralized Claims Protocol
    - Eclipse Conformity Assessment Policy and Cred°ential Profile
    - Eclipse Data Rights Policies Profile (DRP)
- https://gaia-x.eu/
- https://ishare.eu/home/about/the-foundation/
- https://www.velocitynetwork.foundation/

Sovereign by design: Regulatory Compliance and the Cyber Resilience Act

Category: Global, Europe I **Speakers:** Juan Rico (Eclipse Foundation), Daniel Thompson-Yvetot (Tauri), Roman Zhukov (Red Hat) I **Co-organisers hosting this Session:** Eclipse Foundation, DIF

Key takeaways:

1. Compliance is now central to software development for products with digital elements: The definition of "good" software is evolving: compliance with regulatory frameworks like the CRA is as important as performance or security. Early integration of cybersecurity risk assessments and conformity planning is critical to avoid costly rework or legal exposure.

2. Open Source needs representation and stewardship: While casual open source contributors are largely out of scope, open source components used in commercial products must comply. The concept of Open Source Stewards is emerging as a crucial role to help projects meet CRA requirements and support downstream adopters.

3. Understanding roles and responsibilities is essential: Manufacturers, distributors, open source stewards and developers have distinct obligations under the CRA. Companies like Red Hat are mapping these roles and aligning their internal processes—such as due diligence, documentation, and vulnerability management—to meet the regulatory expectations.

4. Collaboration is key to shaping practical open source friendly compliance: Engagement in working groups, standardisation bodies, and community initiatives like the Open Regulatory Compliance WG, CEN/CENELEC, ETSI) is vital to ensure that CRA implementation supports, rather than hinders, the open source ecosystem.

Next steps:

Don't wait, and start developing your compliance path through the following actions:

- Identify the **open source components** you use and whether you're responsible as a **steward** or **maintainer**.
- Track dependencies, vulnerabilities, licensing, and usage contexts to prepare for conformity declarations.
- **Embed cybersecurity risk assessments** into the product lifecycle from the start.
- **Document compliance** measures (e.g., secure design, testing, traceability) early to avoid later requalification.
- Clarify your role for each specific product, component or project, **manufacturer**, **open source steward**, **developer**.
- Assign internal accountability for **CRA readiness**, including legal, security, product, and compliance teams.
- Join industrial initiatives like the **Open Regulatory Compliance Working Group** to work as a community.

Resources:

- Open Regulatory Compliance website: https://orcwg.org/
- CRA FAQ developed by ORCWG: https://github.com/orcwg/cra-hub/blob/main/faq.md
- Presentations: https://github.com/orcwg/orcwg/tree/main/events

Sovereign by design: Trust Frameworks

Speakers: Christoph Strnadl (Gaia-X), Rajiv Rajani (iSHARE), Etan Bernstein (Velocity Network Foundation) I **Co-organisers hosting this Session:** Eclipse Foundation, Ayra

Key takeaways:
Three different approaches for building trust frameworks for data sharing are explained, focusing on the credential and trust part of the process:

Gaia-X presentation
Gaia-X's mission is to establish a trusted, federated data infrastructure standard by developing specifications, rules, policies, and a verification framework, aiming to return data sovereignty to users and enable trusted decentralized digital ecosystems. With over 250 member organizations, including a significant number of SMEs, Gaia-X provides a framework for secure data sharing in global digital supply networks. This framework encompasses technical compatibility, compliance, and labelling, all designed to foster a transparent and interoperable environment that drives the European data economy. Trust frameworks, as exemplified by Gaia-X, are seen as crucial for the efficiency and success of these complex digital ecosystems.

iSHARE presentation
The iSHARE Trust Framework aims to empower organizations with full control over their data by providing a strong foundation for trusted and decentralized data sharing. The iSHARE Foundation, a non-profit entity, is responsible for its evolution, change management, global adoption, and trust governance. The framework addresses the challenge of managing authorizations for data access, especially in complex scenarios with multiple providers, by enabling efficient and sovereign data sharing. It supports various roles, including Data Consumers, Data Providers, Participant Registries, Entitled Parties, and Authorization Registries. The iSHARE framework is being applied in real-world initiatives like the Netherlands Green Deal Data Space for energy reporting and aligns with ISO and EU standardization and regulations such as the Data Act.

VNF presentation
The Velocity Network Foundation is building the Internet of Careers®, an open, public, and decentralized trust framework for career-related credentials. This initiative aims to empower individuals with control over their career records and transform how these credentials are created, stored, and verified. The current labor market infrastructure is siloed and lacks interoperability, leading to inefficient and error-prone processes. Velocity Network addresses this by centering the individual in a verifiable data registry, allowing them to manage and prove their qualifications through digitally signed attestations. The "Sovereign By Design" philosophy ensures individual ownership, consent-based issuing, and minimal data disclosure, while acknowledging the need for issuer revocation rights and credential bundling for certain types of records. This framework is further solidified by a robust governance and legal structure that vets and accredits all participating organizations.

Questions, commonalities and collaboration points
While Gaia-X, iSHARE, and the Velocity Network Foundation each offer distinct trust frameworks, they share the overarching goal of establishing secure and interoperable digital ecosystems by returning data sovereignty to users and fostering trusted data exchange. All three emphasize decentralized approaches, the importance of governance, and the need for robust mechanisms to manage credentials and authorizations. Common ground for collaboration lies in their shared commitment to open standards, transparent operations, and empowering individuals and organizations with control over their data. Notably, Gaia-X and iSHARE are already demonstrating this collaborative spirit through their joint efforts within the Eclipse Dataspace Working Group and the different protocols

being specified there. This shared foundation suggests significant potential for further cooperation among all three initiatives to accelerate the development of a more trusted and interconnected digital landscape.

Next steps:
Additional details and questions are planned for the next session “Sovereign by design - Panel”, where the same speakers will discuss on related questions and dig deeper into certain aspects related to trust and digital sovereignty.

Resources:

- https://gaia-x.eu/
- https://ishare.eu/home/about/the-foundation/
- https://www.velocitynetwork.foundation/

The Recipe for Digital Health Credentials: Technical Standards & Government Experiences for Digital Health Credentials

Category: Africa, Latin America & Caribbean, Europe, Global, Health I **Speakers:** Andrew Kajeguka (East Africa Community Secretariat), Carlos Javier Nuñez Contreras (RACSEL), Konstantin Hyppönen (European Commission – DG CNECT), Jennifer A Nelson (IADB), Garrett Mehl (WHO), Osama El Hassan (Dubai Health Authority) I **Co-organisers hosting this Session:** European Commission, WHO

Key takeaways:

- The session's primary goal was to provide practical insights into the implementation process for Digital Health Credentials, discuss necessary technical standards, highlight challenges, and share real-world government experiences.
- The WHO's approach is guided by the Global Strategy on Digital Health which calls for interoperable systems built on open standards. The strategy for digital transformation is based on a "Full-STAC" of open Standards, Technologies, Architectures, and Content.
- The WHO Global Digital Health Certification Network (GDHCN) acts as a trust framework, functioning like a global "public key" directory to verify the authenticity of credentials without accessing personal health data. Multiple use cases are envisioned, including the International Patient Summary (IPS), childhood immunization records, and COVID-19 certificates.
- The European Commission is developing the European Digital Identity Wallet (EUDI Wallet) as a secure digital tool for citizens to access public and private services. The health use case pilot includes cross-border access to e-prescriptions.
- The Inter-American Development Bank (IADB) and partners are leading the Pan-American Highway for Digital Health (PH4H) to enable the secure and interoperable exchange of health data across the Americas.
- RACSEL (The Latin America and Caribbean Digital Health Network) supports the PH4H with a technical "recipe" that blends key standards. This includes using HL7 FHIR for a foundation, the International Patient Summary (IPS) for secure summaries, WHO-DVC schemas for vaccine proofs, and the GDHCN as the "Oven" for establishing cross-border trust.
- The East African Community (EAC) identified critical ingredients for successful implementation, including: Legal & Regulatory Frameworks, Technical Standards, Data Exchange, Capacity Building, Political Will & Funding, Identity Proofing, and User-Centric Design. Potential use cases in the region include RMNCAH, HIV/AIDS Management, and patient referrals

Next steps:

- Establish a set of core global principles and standards while allowing countries and regions the flexibility to adapt them to unique contexts.
- Identify and address the biggest gaps in the current digital health ecosystem, whether they are technical standards, governance frameworks, a skilled workforce, or public trust.
- Use lessons learned from regional implementations—such as balancing standards with flexibility in the EU, ensuring inclusivity in the Americas , and respecting sovereignty in the EAC —to inform future guidance.
- Focus on building public trust and user adoption for digital credentials, drawing from the experience of initiatives like the Hajj Health Card.

Threat Modeling Digital Wallets

Category: Global I **Speakers:** Simone Onofri (W3C), Tara Whalen (W3C), Amir Sharif I **Co-organisers hosting this Session:** W3C, OID

Key takeaways:
We are here for a quick, early-morning threat modeling session for digital wallets. We represent the Worldwide Web Consortium (W3C), the standardization organization for the web. We've recently started addressing how credentials should be securely used on the web.
I'm Simone, Security Lead at W3C, focusing on user security online.
I'm Tara, Privacy Lead at W3C, handling privacy aspects for web users.
I'm Amir, Security Researcher at FBK, working alongside Simone and Tara, focusing on secure and privacy-preserving credential implementation.
Today, we have a one-hour session. Normally, these sessions could last up to four hours, but today will be quick and focused. Our job is to protect users from threats related to privacy, security, and human rights.

Our agenda covers:
1. **Introductions**
2. **Understanding our focus**: Identifying potential threats
3. **Exploring what can go wrong**: The most interesting part!
4. **Discussing mitigations**
5. **Assessing our effectiveness**

W3C was founded in 1994 by Tim Berners-Lee, aiming to create open standards based on principles of accessibility, internationalization, privacy, and security. Today, we're particularly focusing on privacy and security.
Our main approach is "user first," prioritizing user protection against threats from governments, third parties, and websites.

Threat Modeling Introduction:
Is this anyone's first threat modeling exercise? Great! Who has experience in security threat modeling? Privacy threat modeling? Human rights threat modeling? Excellent.

Threat modeling processes vary by organization; no universal standard exists yet. Typically, it involves:
1. Defining the system model
2. Identifying threats
3. Discussing mitigations
4. Continuously updating the model as threats evolve

Today, we'll use Adam Shostack's straightforward four-question process:
- **What are we working on?**
- **What can go wrong?**
- **What will we do about it?**
- **Did we do a good job?**

What Are We Working On?
We're dealing with web credentials APIs, recently published as recommendations, allowing websites to securely request user credentials stored in digital wallets through browsers.

User Flow Example:

- A browser prompts the user to authorize credential sharing.
- User reviews credentials requested (e.g., name, age verification).
- Users confirm sharing through their wallet, with security warnings if necessary.
- Credentials securely transferred to the website.

System Model:

Our model includes:

- Wallet and browser
- Credential issuer and verifier
- Trust boundaries between wallet and browser
- Presentation protocols and formats (e.g., verifiable presentations)

What Can Go Wrong?

Threat examples include:

- Entity impersonation
- Metadata tampering
- Lack of device lock mechanisms
- Trust registry compromise
- Over-collection of user data
- Push notification vulnerabilities
- Insufficient privacy controls leading to "consent fatigue"
- Improper lifecycle management of data by verifiers
- Excessively sensitive data collection by relying parties
- Detectable patterns allowing user identification
- Man-in-the-middle attacks via intermediaries

Mitigations Discussed:

- Strong cryptographic protections
- Transparent and reusable consent mechanisms
- Regulatory frameworks enforcing minimal data collection
- Trust frameworks clarifying relying parties' identities
- Improved user interfaces to enhance trust and transparency

Conclusion:

Threat modeling is continuous and evolving. Your contributions today are invaluable. Please join W3C working groups for further collaboration:

- Threat Modeling Community Group
- Privacy Working Group
- Security Interest Group

Remember, attackers will always ignore your threat model, continuous vigilance and updates are necessary.

Thank you for participating today!

Next steps:

- Organize an on-line interactive session to continue the Threat Modeling exercise
- Document it in the Threat Model Digital Identities

Resources:

- Slides with the results of the Threat Modeling Session: https://docs.google.com/presentation/d/1st-1pt66B1SA4a5oO3FphopJ-gRtx6AFwpuwrFScc2M/edit?slide=id.g33c8b7c0b1c_2_510#slide=id.g33c8b7c0b1c_2_510
- Meta Threat Model for Decentralized Digital Identities https://github.com/w3c-cg/threat-modeling/blob/main/models/decentralized-identities.md
- EUDI Wallet General threat model paper is available here: https://link.springer.com/chapter/10.1007/978-3-031-89350-6_6
- The link to the results table: https://sites.google.com/view/eu-digital-identity-wallet/home
- EUDI Wallet Secure Storage Threat Model paper is available here: https://link.springer.com/chapter/10.1007/978-3-031-96590-6_15
- This is again the link to the additional materials: https://st.fbk.eu/complementary/DBSEC2025
- Identity & the Web Report: https://www.w3.org/reports/identity-web-impact/

W3C Linked Web Storage (LWS)

Category: Global I **Speaker:** Jesse Wright (Open Data Institute) I **Co-organisers hosting this Session:** LF Decentralized Trust, DIF, W3C

Key takeaways:

What are your use cases for Web Attached (Credential) Storage:

1. Analog <-> digital credentials. Systems where issuer uploads PDF file to some kind of storage
2. Membership card in Zurich. Scan PKPass get derived credential that is issued
3. Access of salary statements for tax purposes
4. Using credentials from LWS for log-in
5. Dataspaces - not currently handling personal data. Looking to implement a Pod for all of the personal data that is being handled. ODRL already handled in dataspaces.
6. Higher learning: Point of failure for data retrieval at present. Open-source software developers don't often provide services - and so can't be the host of credentials, passes or other data in general. And transition between analog and verified credential within the context of allowing students to share credentials (PDFs, JSON) with employers.

What similar solutions exist / what are the overlaps+gaps you see:

- OIDC4VP/OIDC4VC
- Formal Specification of "Storage APIs" (Kenny Paterson, Matilda Backendal, Miro Haller et al
    - https://eprint.iacr.org/2024/989
    - https://mirohaller.com/posts/2024/08/e2ee-cloud-storage-security-notions

Next steps:

- join the Linked Web Storage Working Group & join the Solid Community Group
- support the Solid Project at ODI

Resources:

Linked Web Storage Working Group (WG)

- Home: https://www.w3.org/groups/wg/lws/
- Charter: https://www.w3.org/2024/09/linked-web-storage-wg-charter.html
- Solid Community Group (CG): Home: https://www.w3.org/groups/cg/solid & Solid at the ODI: Contact: solid@theodi.org

---

What would it take for global acceptance of the W3C's Digital Credentials API?

Category: Global I **Speakers:** Simone Onofri (W3C), Heather Flanagan (Spherical Cow Consulting) I **Co-organisers hosting this Session:** W3C, OpenID

Key takeaways:

Introduction

At its core, the DC API is extremely small (the interface itself is only about seven lines of code), yet the overall specification, with its privacy considerations and threat mitigations, runs much longer. Our goal today is to explain precisely what this "tiny API" does, and then surface where people worry it might fall short.

What the DC API Actually Does

- **Seven-line interface**: From the spec you'll see only a handful of method signatures (the "green arrows" in Tim's diagram).
- **Purpose**: It moves a JSON payload securely from the browser's JavaScript context into the native platform layer (and back), enabling the browser and the wallet to exchange structured credentials.
- **Privacy & Security**: All sensitive data is end-to-end encrypted. The API itself is a "dumb pipe"—it cannot inspect or modify the credential contents.

Common Flows

1. **Same-Device Flow**
    - The browser and the wallet both live on the same device.
    - The API simply marshals a JSON blob in and out of the user agent.
2. **Cross-Device Flow**
    - The website displays a QR code (or deep-link) that the user scans with their wallet app.
    - That triggers the platform's native DC API on the other device, again shuttling the same JSON through encrypted channels.

Work in Progress

- **W3C Federated Identity Working Group**
    - **FedCM stream**: Federated Credential Management API.
    - **DC API stream**: Our focus—digital credential presentation.
- **First Public Working Draft** (FPWD)
    - Published yesterday as a "line in the sand."
    - Invites implementers and IP stakeholders to review and comment now, before the spec solidifies.
- **Ecosystem Threat Modeling**
    - Parallel work in the W3C Threat Modeling Community Group is mapping out broader privacy and security risks.
    - Both streams inform each other: DC API must slot into an ecosystem of wallets, RPs (Relying Parties), and registries.

Early Implementations & Feedback

- **OpenID for Verifiable Credentials (OID4VC)** already references and will point to our FPWD.
- **Google** ran an Origin Trial beginning August 2024, gathering real-world feedback.
- **Apple** enabled the API behind a feature flag in February 2025.
- **Next steps**: See the GitHub repository via the QR code on the slide to file issues—especially around registry requirements, encryption, or consent flows.

Discussions for adoption

1. **Registry as Gatekeeper**
    - If protocol registries become mandatory, countries or organizations may refuse to participate ("Western techno-colonialism").
    - **Open question**: Can we allow non-registry-based interactions, or at least multiple registries?
2. **User Consent & Prompts** (Sarven & Esther)
    - **When** and **where** should the user be asked for permission?
    - Should that live in the browser UI, the wallet UI, or both?
    - EU regulation places much of this responsibility on the wallet provider.

Native & Web-View Integration

- **Native Apps** (Leya Yang)
    - A passkey-style API makes it easy for verifiers to call the same interface in a native SDK or WebView.
    - Android already supports this "same-API" approach.
- **Web Wallets Debate**
    - Should we exclude pure web-based wallets?
    - Political considerations: control over credential issuance and verification.

User Choice & Trust Models

- **Multiple Wallets**
    - Just as we carry multiple physical cards, users should choose among digital wallets.
    - Branded, government, or native-app wallets might coexist on one device.
- **Browser as Middleman**
    - A QR-code side-channel gives wallets and browsers a direct encrypted link, bypassing untrusted servers.

Presentation vs. Authorization

- **Presentation Only**
    - DC API is explicitly **not** for authorization or authentication.
    - It transports encrypted attributes; it does not handle signatures, long-running sessions, or contract negotiations.
    - **CTAP hybrid** flows (USB or cable) still require a rendezvous server—outside the DC API's remit.

Threat Model Highlights

- **Trust Boundaries**
    - Can we trust the OS, the browser sandbox, or the wallet app itself?
- **Metadata Exposure**
    - Even the list of credential types or sizes can leak sensitive information.
- **Malicious Relying Parties**
    - We must protect RPs from accidental data leaks and hold them to privacy-by-design.
- **Cross-Device Attacks**
    - QR-code spoofing or relay attacks are mitigated by encrypted side channels (e.g. Alicia).

Sovereignty & Political Neutrality

- **European Sovereignty**
    - Governments want assurance that their nationals' credentials won't flow through U.S.-controlled servers.

    - Some standards bodies worry about undue influence by large tech companies.
- **Political Agnosticism**
    - The DC API spec stays strictly technical: no policy rules about which wallets must be used or who runs them.
    - Instead, it provides the building blocks; implementers balance security, privacy, and local regulations.

Usability & "Pit of Success"
- **Lazy RPs & Users**
    - Verifiers want "it just works" with minimal integration effort.
    - Users want one-click credential sharing—yet need safeguards against over-sharing.
- **Defining "Success"**
    - Is success purely a completed transaction?
    - Or must we ensure every step meets privacy, security, and consent standards?
    - The answer varies by use case (e.g. booking a train ticket vs. sharing medical records).

Next steps:
We'll continue this conversation in the W3C community group and on GitHub. Your issues, your code contributions, and your critical feedback will shape the API as it moves from draft to recommendation.

- **Registry Flexibility**: Can we support multiple registries or opt out entirely?
- **Consent Ownership**: Browser UI vs. wallet UI vs. government oversight?
- **Protocol Security**: Mandatory encryption and signing of requests?
- **Wallet Diversity**: How do we interoperate wallets from different vendors and jurisdictions?
- **Authorization Flows**: If a verifier needs a long-running, authenticated channel, how do they bootstrap it from the DC API?

Resources:
- Slides https://docs.google.com/presentation/d/1ZcIJk-AtBwuiqe5WFBkbNj5TLVwaV1IIVvVLWAdUTNg/edit
- Digital Credentials API https://w3.org/TR/digital-credentials

---

What's new in W3C Verifiable Credentials?

Category: Global I **Speakers:** Pierre-Antoine Champin (W3C/Inria), Brent Zundel (Tradeverifyd) I **Co-organiser hosting this Session:** W3C

Key takeaways:
The VC working group at W3C has recently published 7 new standards and 2 candidate standards.
A credential is composed of a set of claims about a subject (such as "this person's birthday is X"), metadata about the credential itself (such as who issued the credential and when), an "proofs" (that make the credential verifiable). When the holder presents their credentials to a verifier (a relying party) they use a "verifiable presentation" - which contains (pieces of) credentials (e.g. for selective disclosure, or bundling several credentials about the same subject), its own metadata and proofs. The proofs of the presentation are provided by the credential holder. VCs and VPs are serialized in JSON-LD, and therefore can be interpreted as pure JSON or as a linked data graph using JSON-LD tools. There is work going on to define a CBOR representation.

Specs: VC Data Model; JSON Schema; Controlled Identifiers; Embedded proofs (Data Integrity suite - signed RDF data graphs using existing signature tech - EdDSA, ECDSA, BBS) or enveloping proofs (JOSE and COSE from IETF); Bistring status list.

7 of these specifications were released as W3C Recommendation in May 2025 and are already referenced by the eIDAS specs (EU regulation). The last 2 are done from the point of view of the working group, but are pending on external factors to become Recommendation (lack of implementation feedback for JSON Schema, waiting for the stabilization of the BBS algorithms).

Question: why use W3C credentials rather than other credential formats? A: no single format can work for everyone. The benefits of W3C VCDM comes from linked data aspect, e.g. the possibility to reuse existing largely accepted ontologies or controlled vocabulary. An example is given in global commerce, as well as a VC-powered bills-of-lading in use in Singapore.

Question: is the licence of W3C standards another differentiator? A: Yes, all W3C Recommentation are openly and freely available and published under a royalty-free license, which fosters multiple interoperable **open source** implementations.

Question and discussion about non-personal attestations - e.g. a car that belongs to more than one person, or a credential associated with a child who needs to be administered by / delegated to the child's parents or legal guardian. Seems like a gap currently - but a general gap rather than a W3C Verifiable-Credential-specific gap. This is sometimes called "trust framework" - how different credentials and issuers fit together. VCs allow you to "link" credentials to make linked claims about things.

Question: do we need to do something else to do ZKP? A: we already have JOSE and CSE that use ECDSA - and that is the input to the Longfellow system that enables ZKP, so short answer is no.

Question: can we expand this to domain names? DNS already has a lot of this... e.g. DNS-SEC. A: one way to leverage DNS and DNS-SEC would be to create a new sub-specification ("cryptosuite") of Data Integrity using DNS-SEC.

Next steps:

- Work on rendering of VCs, and confidence method for external resources
- Confidence-method-specification: e.g. embedding a photograph into a VC is cumbersome. But embedding a link and signing a hash of the linked content makes it more streamlined. This needs to be specified.
- Work in the FedID working group on an API that let web applications interact with a wallet (work in progress: First Public Working Draft just published). "The trust framework layer is underdeveloped compared to the rest of the pieces."

Resources:

- W3C VC overview: https://www.w3.org/TR/vc-overview/
- W3C Digital Credentials API draft spec: https://w3.org/TR/digital-credentials

Closing with honorary guest Federal Councillor Jans

Youtube: Link I **Article:** Link

Federal Councillor Beat Jans delivered the closing address of the conference, acting as host on behalf of the Swiss Confederation. Federal Councillor Jans began by expressing Switzerland's heartfelt appreciation for the attendees' presence, insights, and extraordinary dedication, acknowledging the impact achieved. He further noted that organising such an event with over 40 Co-organisers with all having equal rights and voices, meant navigating a truly collaborative and sometimes complex and frustrating process – reminding him the daily work of the Federal Council.

Federal Councillor Jans emphasized that this conference has not only focused on technical aspects but has also reaffirmed the human values at the core of identity, namely dignity, autonomy, consent, and trust, which must guide all technical and regulatory decisions. He stated that although these words are often used loosely, they are essential values that guide his thinking and actions and sees the responsibility to uphold these values in every decision as a compass. He feels confident that this compass is also shared by many of the conference participants.

The conference discussions are deeply timely for Switzerland. The Swiss parliament has passed an eID act based on the following approach: public issuance, open standards, and a commitment to transparency. About 56,000 citizens have requested a referendum on the new act, and on September 28, 2025, Swiss citizens will vote to approve or reject the eID. He expressed confidence in its approval, because the process used by the Federal Office of Justice to develop the project was inclusive, transparent, and democratic. He also recognizes that concerns expressed must be taken seriously and that the best way to confront them is through events like the Global Digital Collaboration Conference, where experts can address these issues in a transparent fashion.

Federal Councillor Jans concluded by stating that Switzerland takes the responsibility to keep the momentum that the conference has built up going. He emphasized, however, that this a global effort requiring shared responsibility and deepening partnerships, as no country can do this alone.

Outlook

Following the overwhelmingly positive feedback from the participants received during the Conference and the positive results from the survey that was sent afterwards, the Global Digital Collaboration Conference will take place again next year. The Global Digital Collaboration Conference 2026 will take place on September 1–3, 2026, at Palexpo, Geneva.

As Federal Councillor Beat Jans mentioned in his closing remarks, we're planning to expand the governance structure of the GDC. Work on this is well underway, and we look forward to sharing more details, along with information on how to register for the 2026 edition, as soon as possible.

Follow the news on LinkedIn and check the website regularly to stay up to date. Also, feel free to subscribe to our newsletter to receive the latest information in your inbox. Lastly, you can find all pictures from the event here.

See you next year, and let's collaborate in-between!

Thank you very much!

Annex 1: List of Co-organisers

The following Organisations co-organised GDC25 (in alphabetical order):

- American Association of Motor Vehicle Administrators (AAMVA)
- Association of European Vehicle and Driver Registration Authorities
- Austroads
- Ayra
- Blockchain Governance Initiative Network (BGIN)
- Car Connectivity Consortium (CCC)
- Center for Digital Public Infrastructure (CDPI)
- Cloud Signature Consortium (CSC)
- Decentralized Identity Foundation (DIF)
- Digital Credentials Consortium (DCC)
- Digital Credentials for Europe (DC4EU)
- Digital Identity and Data Sovereignty Association (DIDAS)
- Digital Impact Alliance
- Digital Society
- Eclipse Foundation (Eclipse Foundation)
- Ecole Polytechnique Fédérale de Lausanne Center for Digital Trust (C4DT)
- European Commission (EC)
- European Committee for Electrotechnical Standardization (CENELEC)
- European Telecommunication Standards Institute (ETSI)
- European Wallet Consortium (EWC)
- Fides
- FIDO Alliance
- Fintech Open Source Foundation
- Generative AI Commons
- Global Legal Entity Identifier Foundation (GLEIF)
- Global Trust Foundation (GTF)
- GlobalPlatform
- International Electrotechnical Commission (IEC)
- International Federation of Red Cross and Red Crescent Societies (IFRC)
- International Organization for Standardization (ISO)
- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF)
- iSpirt
- Linux Foundation (LF)
- Modular Open Source Identity Platform (MOSIP)
- Nordic Baltic EID project
- Open ID Foundation (OID)
- Open Mobile Hub (OMH)
- Open Wallet Foundation (OWF)
- Organization for Economic Cooperation and Development (OECD)
- POTENTIAL
- Project Liberty Institute
- Tazama
- United Nation High Commissioner for Refugees (UNHCR)

- United Nations Conference on Trade and Development (UNCTAD)
- United Nations Economic Commission for Europe (UNECE)
- United Nations International Computing Center (UNICC)
- Verifiable Trade Foundation (Verifiable.Trade)
- World Bank Group (WBG)
- World Health Organization (WHO)
- Worldwide Web Consortium (W3C)

Annex 2: List of Day 2 Sessions

Title	Speaker(s)	Description	Co-organiser(s)
A Smart Health Wallet: Privacy & Control in Your Hands Tags: Global, Health	Carl Leitner (WHO), Jason Taylor (Google), Alan Stapelberg (Google), Grahame Grieve (HL7), Konstantin Hyppönen (European Commission - CNECT)	Demonstration of a Health Wallet prototype showing secure carrying, presenting, and verification of digital health proofs (e.g., vaccinations, record links) using open standards. Followed by a discussion on the practical application and importance of selective disclosure for user privacy.	European Commission, WHO
Achieving global interoperability for digital wallets by profiling OpenID4VC over DC API (HAIP) Tags: Global	Lee Campbell (Google), Tim Cappalli (Okta), Christian Bormann (SPRIND), Oliver Terbu (Mattr), Kristina Yasuda (SPRIND)	To realize secure and interoperable digital wallets, a lot of different building blocks need to play together. This session shows how technical standards and a profile thereof allows for interoperable implementations. A live demonstration and explanation of the OpenID For Verifiable Credentials protocols, the W3C Digital Credentials API, and fido CTAP according to the OpenID High Assurance Interoperability Profile shows how the different building blocks fit together.	fido, W3C, ISO, OpenID, IETF
Advancing Digital Identity in Korea: Scalable Infrastructure, Privacy Innovation, and Global Expansion Tags: Asia & Oceania, eGovernment	Sanghwan Park (Korea Internet & Security Agency (KISA), Ace Shim (Hopae), Wonseok Baek (Samsung Electronics)	Building on the high-level overview presented on Day 1, this deep-dive session will explore South Korea's integrated public-private efforts to develop and deploy secure, privacy-preserving, and interoperable digital identity and wallet solutions. The Korea Internet & Security Agency (KISA) will present the national policy framework and evolving technical infrastructure supporting trusted digital credentials. Hopae will share the design principles, privacy architecture, and operational challenges of COOV, a decentralized wallet that served over 43 million users and achieved interoperability with the EU and Singapore. Samsung will outline its role in implementing mobile ID credentials through Samsung Wallet and its strategy for enabling private-sector and international applications of digital identity. This session will highlight key lessons in policy design, technological architecture, and cross-sector governance, offering insights for countries and organizations seeking to scale digital identity systems with both trust and flexibility.	ITU
Agentic AI and Digital ID Tags: Global, Payments, Digital assets	Wenjing Chu (Futurewei Technologies), Scott Perry (Digital Governance Institute), Andor Kesselmann (Ayra, DIF), Eric Drury (ForthCo.io)	As AI agents act increasingly autonomously and AI-generated content expands rapidly, we face new trust challenges. Starting with an overview of the AI standards landscape, this session addresses critical needs including establishing trust protocols for AI agents and verifying authentic content. We'll discuss decentralized identity solutions for these challenges, with actionable implementation strategies.	Decentralized Identity Foundation, LF Decentralized Trust
AI for Humanity: Agentic AI Tags: Global, Digital signatures, Drivers licence, Organizational credentials, Car keys	Wenjing Chu (OpenWallet and LFDT), Drummond Reed (the First Person Project), Scott Perry (Digital Governance Institute), Eric Drury (ForceCo.io)	Agentic AI – Autonomous AI Agents and Human Trust: :: The Rise of AI Agents and How We Can Trust Them :: The Future of Human Identity: The First Person Project :: How Can We Trust What We See Online in the Agentic Web?	ITU, Ispirt
AI for Humanity: Maturity and Evaluation	Dong Sun, Ethan Westfall IEEE AI working group	AI Maturity and Evaluation – developing a common framework and an AI maturity index aligned with human well-being values: :: Debrief the challenges of measuring AI benefits :: International Collaboration for AI Testing :: Open Discussion	ITU, Ispirt

AI for Humanity: Open Model Collaboration Tags: Global	Yonghua Lin (BAAI), Anni Lai (Generative AI Commons), Harshit Kacholiya (Sunu Engineer/iSpirit)	Open Model Collaboration – advancing transparency, interoperability, and innovation through open models: :: Democratizing AI for Global Challenges :: Model Openness Framework :: Open Discussion	ITU, Ispirt
AI for Humanity: Responsible AI Tags: Global, Africa, Asia & Oceania, North America, Latin America & Caribbean	Anni Lai (Generative AI Commons), Rob Geada (Redhat), Harshit Kacholiya (Ispirit), Vijay Mauree (ITU)	Responsible AI – embedding ethics, safety, and governance at every layer of AI development: :: AI for Humanity Program Introduction :: Responsible Generative AI Framework :: Trusty AI :: AI Child Safety – Harshit Kacholiya, :: AI and Multimedia Authenticity :: Open Discussion	ITU, Ispirt
AI for Humanity: Social and Economic Impact Tags: Global	Sachiko Muto (OFE/Rise), Dylan Reim (World Economic Forum)	AI for Humanity: AI's Social and Economic Impact – understanding and addressing AI's implications for labor, equity, and access	ITU, Ispirt
Alternate Payment Rails: Delivery of Funds in Emergency Scenarios	Ani Popiashvili (WBG)	This session explores how blockchain-based digital currencies can help ensure the continuity of financial operations during emergency situations, particularly in Fragile, Conflict, and Violence (FCV) settings. As part of a collaborative initiative, the session will present key findings that inform the design of a prototype end-to-end payment solution—built on a layered technology stack that includes blockchain infrastructure, stablecoins, and digital service platforms—to support both emergency and operational disbursements.	World Bank Group
Blockchain's Role in Global Digital Collaboration Tags: Global, Humanitarian, Payments, Digital assets	Daniela Barbosa (LF Decentralized Trust), Paul Wong (Stellar Foundation), Pratheep Ponraj (The World Bank), Steffen Schwalm,	This session explores how blockchain-based identity and wallet solutions are being deployed to address real-world challenges in humanitarian aid, development finance, and cross-border business. It will include three talks on the practical implementations of blockchain identity addressing global challenges. Talk 1: Practical lessons from deploying digital wallets to support payments in humanitarian and development settings from the Stellar Foundation drawing on the experiences of UNHCR and GIZ. Talk 2: Learn how FundsChain—the World Bank's blockchain platform—brings real-time transparency and accountability to development project funding. Launched in 2024, it enables governments, donors, auditors, and beneficiaries to track disbursements, verify documents, and monitor how funds are used through a secure, tamper-proof system. Talk 3: Overview of the B2B & EU Business Wallet.	LF Decentralized Trust, DIF
Blockchain's Role in Global Digital Collaboration - Foundations Tags: Global	Daniela Barbosa (LF Decentralized Trust), Hendrik Ebbers (Hashgraph/Hedera), Kim Duffy (DIF), Heather Dahl (Indicio)	Intro to Blockchain's Role in Global Digital Collaborations plus two talks : Talk1: Talk exploring how pioneering deployments of verifiable credentials in travel, finance, and education are transforming identity systems—delivering real-world benefits today while shaping the digital trust infrastructure of tomorrow. Talk 2: Blockchain-based Decentralized Identity and Trust from the Ground: Building Secure and Interoperable Digital Identity on Open Infrastructure	LF Decentralized Trust, DIF
Breaking and Fixing Idenity Protocols with Formal Analysis Tags: Global	University of Stuttgart (Fabian Hauck and Pedram Hosseyni)	As digital identity systems grow more complex and critical, ensuring their security demands more than expert reviews and penetration testing. In this talk, we give an introduction to formal security analysis - a rigorous, mathematical approach to protocol security evaluation - and explain how it complements traditional methods. We'll present the Web	OpenWallet Foundation, OpenID

		Infrastructure Model, a proven methodology applied to widely deployed protocols like OAuth 2.0 and OpenID Connect, and now to emerging wallet-based standards such as OpenID for Verifiable Presentations. Real-world case studies will show how formal analysis has uncovered and helped fix critical vulnerabilities before deployment, highlighting its value in building trustworthy identity ecosystems.	
Bridging Governance and Technical Design: DSNP at the Crossroads of Open Ecosystems Tags: Europe, North America, Digital signatures, Digital assets	Alberto Leon (Harvard's Applied Social Media Lab), Sarah Nicole (Project Liberty Institute), Wendy Seltzer (DSNP), Wes Biggs (Project Liberty)	Technical design choices and governance models directly influence each other. In decentralized systems, navigating this interplay is even more complex and critical. In most projects, technical choices and governance both work in complete silos and more often than not governance is an afterthought. Drawing from use cases like age verification, wallet-based identity, and decentralized social networking, this session we will discuss paths to help bridge technical and governance perspectives, support interoperability, and foster open social and identity ecosystems that work seamlessly for developers and users. The Decentralized Social Networking Protocol (DSNP) is one example that raises these questions in practice. The session will use it as a reference point to explore how technical specifications and governance considerations can evolve together, and what it takes to build protocols that can support coordination across diverse communities and systems.	Project Liberty Institute, Harvard Applied Social Media Lab
Bridging the Organizational Identity Gap: From Nano-Businesses to Global Commerce Tags: Global, eGovernment	Ivan Mortimer-Schutts (GLEIF), Darrell O'Donnell (Ayra), Pramod Varma (CDPI), Goran Vranic (WB), David Porteous	Organizational identity is critical for commerce, with formal systems like Legal Entity Identifiers (LEI) providing essential linkages into the broader economy. However, nano- and micro-businesses face a significant gap—they need scalable organizational identity but lack clear incentives or resources for complex formal processes. This session explores how to create stepping-stone solutions that help smaller organizations build toward formal identity systems without overwhelming administrative burden.	CDPI, Ayra, World Bank Group
Building an EUDI Wallet, and the lessons learned when using it for Qualified Electronic Signatures. Tags: Global, eGovernment, Organizational credentials, Digital signatures	Ana Gossens (Animo), Melanie Moreno (DocuSign)	In this session Animo shares how they built their EUDI wallet prototype on the open-source framework Credo. They discuss the required and advanced EUDI features and give a demo of their wallet. The session will then dive into one specific innovation, namely Qualified Electronic Signatures. DocuSign joins as a co-host to discuss the benefits, challenges, and next steps in utilizing the EUDI wallet for QES processes. Animo and DocuSign share their collaboration on a proof of concept for a QTSP-centric integration with the EUDI Wallet.	OpenWallet Foundation, FIDES
Building and Scaling ID Solutions for UN and Governments Tags: Global, Humanitarian, Payments, Organizational credentials	Emily Bennett/Dimitra Ralli (UNICC), Massimiliano Merelli (UNiD), Sean Bohan (OWF), Hart Montgomery (LFDT)	UNICC will share its journey in developing scalable digital ID solutions for the UN system and government partners. The presentation will highlight the foundational inputs, technical specifications, and the process of reaching MVP, as well as the roadmap for expanding the capabilities of these solutions. The discussion will also cover UNICC's work in decentralized identity products, including the integration of biometric identification, tailored to the needs of both UN entities and national governments.	UNICC, LF Decentralized Trust, OpenWallet Foundation
Charting the Course: National Digital Health Wallet Use Cases Tags: Africa, Latin America & Caribbean, Asia &	John Mark Esplana (IFRC), Steven Wanyee, (HELINA Africa), Osama El Hassan (Dubai Health Authority), Erick Kitali (Tanzania Government), Matthew Keks	Explore diverse use cases and real-world country experiences with government-led health digital wallets. The session focuses on analyzing lessons learned (successes, challenges) from these examples and integrating these practical insights to build more effective, context-specific implementation roadmaps.	WHO, IFRC

Oceania, Health, Humanitarian	(WHO), Roberta Andraghetti (WHO)		
Citizen Wallets and Payment: virtuous cycle of identity and payments in a government wallet Tags: Global, Payments, eGovernment, Organizational credentials	Ranjiva Prasad (Visa), Piers Clough (Visa) Panelists: Selamawit (Selam), Reta (Government of Ethiopia), Helge Michael (Lissi), Maurizio Fatarella (PagoPA), Machiel van der Harst (Tech5), Marie Austenaa (Visa)	This panel, hosted by Visa and the Open Wallet Foundation (OWF), explores the intersection of digital identity and payments in citizen wallets. Featuring leaders from the public sector, technology, and digital identity fields, the discussion will examine how integrating secure payments and digital identity in citizen wallets can create a "virtuous cycle" of adoption and utility. Panellists will share global perspectives and lessons learned from large-scale government identity programs, discuss the role of standards and interoperability, and highlight how public and private sector collaboration can drive greater inclusion, efficiency, and security in digital public services. The session will also consider concrete use cases and success factors for deploying citizen wallets, with audience Q&A to follow.	LSPs, OpenWallet Foundation
Conformance tests (Standards track) Tags: Global	Joseph Heenan (Open ID Foundation)	The OpenID for Verifiable Credential specifications (OID4VCI, OID4VP & HAIP) have been widely adopted - but how do you ensure that people are implementing the specifications correctly so that both security and interoperability is achieved, allowing ecosystems to scale quickly and with lower risk? Joseph introduces the semi-automated protocol conformance tests that the OpenID Foundation has developed, explains their strengths and scope, does a live demo of testing issuers, wallets & verifiers, and talks about how regulators & ecosystems can adopt OpenID Foundation certifications.	OpenID Foundation
Cross-Border Interoperability: Initiatives, Challenges, and the Road Ahead Tags: Asia & Oceania, Europe, North America, Global, Drivers licence, Trade, Digital travel, eGovernment	Antony Carmoy (France Titres, France), Aristide Adjinacou (Agence nationale d'identification des personnes (ANIP)), Charlie Smith & Michael Animashaun (Department of Science, Innovation and Technology, United Kingdom), Connie LaSalle (NIST, United States), Laura Aydinyan, (Information Systems Agency, Armenia), Vicente Navarro (DG Connect, European Commission), Cecilia Emilsson (OECD), Adam Cooper (World Bank)	This session will explore real-world initiatives and experiences in advancing cross-border interoperability of digital identity systems. Through a series of short presentations, government and international experts will spotlight recent or ongoing efforts from around the world, offering insights into their goals, approaches, and early results. A moderated panel will then dive into the core challenges these initiatives have faced—legal, technical, institutional—and explore what tools or reforms could help overcome them. With perspectives from Armenia, Benin, the EU, France, UK, US, OECD and the World Bank, the discussion aims to identify practical lessons and spark ideas for stronger bilateral and multilateral collaboration moving forward.	OECD, European Commission, LSPs, World Bank Group
Decentralized Identifiers (DIDs) for global interoperability (Standards Track) Tags: Global	Markus Sabadello	In any digital identity system, different types of identifiers are used for referring to individuals, organizations, and things. Identifiers are an essential basis for higher-level components such as credentials, wallets, and agents. Today, identifiers are often based on hierarchical technical infrastructures or issued by central authorities. In contrast, this session explains the motivation behind the Decentralized Identifiers (DIDs) standard, and proposes that the decentralized nature of DIDs greatly facilitates the vision of global interoperability.	DIF, W3C
Decentralized Identity: The View from the Market	Ulrike van Venrooy (EY), Florian Kohlar, (KPMG) Martin Kuppinger (KuppingerCole Analysts)	In this session, experts from KPMG and EY will discuss with Martin Kuppinger about the feedback from the broader market on decentralized/digital identities. They will look at how organizations are looking at the possibilities of these technologies across a variety of use cases, including digital	DIF, OpenWallet Foundation

		product passports, consumer-centric use cases, and enterprise use cases. This discussion will provide insights into whether organizations already are aware of the potential that decentralized identities provide for improving business models and business processes, including entering new fields of business. They also will look at what is needed in dissemination to attract organizations at scale to invest into decentralized identity as part of their modern IT ecosystems.	
Deep Dive session on Digital Travel Credentials: Policy focus Tags: Latin America & Caribbean, eGovernment, Digital signatures	Annet Steenbergen (EWC/Circletree), Ciran Carolan (ICAO), Gabriel Marquie (IATA), Laurent Loup (EWC/SICPA), Leire Bilbao (Visit Benidorm), Lisette Looren De Jong (NL Government – Ministry Justice & Security), Florent Tournois (Aptitude)	The world of travel and hospitality has public and private stakeholders responsible for setting regulation and the operational compliance with regulation. The ICAO DTC is a standard set with the border authorities in mind. Airlines and hotels often need to comply with regulation that states verification and data from a travel document is required. Often this conflicts with data privacy regulations like data minimization. By showcasing pilots and PoC's that use the DTC this session will focus on discussing what is needed to achieve digital global interoperability for digital travel credentials.	LSPs, OpenWallet Foundation
Deep Dive session on Digital Travel Credentials: Technology focus Tags: Global, Digital Travel	Annet Steenbergen (EWC/Circletree), Laurent Loup (EWC/SICPA), Maarten Boender (4Sure), Ciaran Carolan (ICAO), Anthony Carmoy (Aptitude), Siddharth Sharma (Digi Yatra), Gabriel Marquié (IATA), Ramesh Narayanan (MOSIP), Arjan Geluck (ISO)	A few key technical enablers need to be aligned in order to achieve global interoperability and trust across jurisdictions and industries to implement travel use-cases. Various eco-systems and industries have their own approaches and need to converge to a common set of features (notably credentials formats, protocols and trust registries).	LSPs, ISO
Demo Hour - Wallet Apps	Kristina Yasuda (DE), Anthony Carmoy (FR)	This session shall give room to demonstrations of real world wallets (either already deployed or under development): - FR national wallet - DE national Wallet - CH SWIYU - City of Kyiv - Diia - Singapore	LSPs, World Bank Group, OpenWallet Foundation, CDPI
Digital business registries supporting growth and transparency Tags: Global	Frank Grozel (UNCTAD), Clare Rowley (GLEIF), Kjartan Sorenson (UNITAR)	Business registries have an important role to play in simplifying and digitalising company creation, not just for company registration but to help investors obtain all the mandatory registrations and permits they need to get up, running and producing Done well this has a positive economic impact, with more companies created, more investment into the economy, greater formalisation, a stronger SME sector, diversified ownership and higher levels of employment. It also provides valuable data for governments to better manage the economy, makes it easier for companies to obtain loans and provides transparency on beneficial ownership to combat fraud.	UNCTAD
Digital ID in Africa: Foundations for Inclusive Digital Transformation through DPI Tags: Africa	Gabi Adotevi (MOSIP), Rahel Yitbarek (NID - Ethiopia), Aristide Adjinacou (ANIP - Benin), Antony Muriiti (CDPI), Abisoye Coker-Odusote (Nigeria)	As Africa marches towards the digital future, digital ID systems are becoming foundational elements of Digital Public Infrastructure (DPI), enabling inclusive access to services, governance, and economic opportunities. Several African countries are moving beyond traditional ID systems to reimagine digital identity as a shared public good which is interoperable, inclusive, and rights-based. This session, hosted by MOSIP, brings together policymakers, technologists, and global development partners to explore how the continent is shaping next-	MOSIP, CDPI

		generation digital ID ecosystems. It will examine how countries are integrating DPI principles, such as openness, modularity, and trust, in the design and implementation of their identity systems.	
Digital Inclusion of SMEs in LAC with VC	Yolanda Martinez (WBG), Armando Manzueta (MAP, DR), Sovieski Naut (ABA, DR)	Launching of the pilot of Verifiable Credentials in the Dominican Republic and round table with LAC Countries and development partners.	World Bank Group,CDPI
Digital Sovereignty	Paolo de Rosa (European Commission), Pablo Chavez (CNAS), Pramod Varma (CDPI), Jennifer Tridgell (University of Cambridge), Gab Columbro (Linux Foundation Europe)	This session examines how countries and regions are seeking to assert strategic autonomy in the digital age. Rather than pursuing isolation or pure self-sufficiency – and perhaps counterintuitively – many are turning to cooperation, interoperability, and shared infrastructure as a means of building digital autonomy, resilience, and competitiveness. As reliance on foreign platforms and AI models exposes structural vulnerabilities, the panel will explore how open-source technologies, collaborative AI development, digital public infrastructure (DPI), and harmonized standards can together form the foundation of a new model of digital governance that promotes sovereignty while maintaining an international digital ecosystem. This emerging approach – often described as "digital cooperation" or "digital solidarity" – may offer a more resilient, democratic, and multilateral path to digital sovereignty, while steering clear of zero-sum or isolationist impulses.	European Commission, CDPI, OpenWallet Foundation
Digital Wallets in Action: Sustainable Cities - Global Interop Track Tags: Global, Organizational credentials, eGovernment, Trade, Education	Harmen van der Kooij (FIDES Labs, Vicor van der Hulst (FIDES Labs), Nikos Triantafylou (University of Aegean) Ramesh Narayanan (MOSIP), Ana Goessens (Animo), Sean Bohan (Open Wallet Foundation)	This session introduces the FIDES Community, an open, global initiative accelerating adoption and interoperability of digital wallets and verifiable credentials. It highlights the Sustainable Cities Track, with live demos showing how compliant personal and organizational wallets enable use cases like procurement and recruitment. We also present the Open Test Bed and conclude with reflections from OWF, MOSIP, and Animo, plus a short Q&A.	FIDES, MOSIP, OpenWallet Foundation
Digital Wallets: Architecture, Interoperability and Industry Outreach Community Spotlight: Forkbomb Discussion and Demo Tags: Global, Digital signatures, Organizational credentials	Char Howland (Indicio), Carla Jedani (thepass.id), David Alexander (Mydex), Andrea D'Intino (Forkbomb)	Join us for an engaging session highlighting the Special Interest Groups (SIGs) within the OpenWallet Foundation (OWF). Each SIG will present its purpose, current initiatives and opportunities for community involvement. Following the SIG updates, community member ForkBomb will share insights into their project. This session offers an opportunity to learn about the diverse activities within OWF and discover how you can engage and contribute.	OpenWallet Foundation, LF Decentralized Trust
e-democracy, e-topia Part 1 Tags: Global, Digital signatures, Digital assets, eGovernment, Democracy	Olga Baranova, Laetitia Ramelet, Andrzej Nowak, Grégoire Barbey, Imad Aad, Katherine Loh	As democracies increasingly depend on digital services—like e-identities, e-voting, and e-collecting—new opportunities arise alongside risks such as fraud, privacy loss, and misinformation. The Center for Digital Trust (C4DT) at EPFL is seeking co-contributors for a session exploring the foundations and challenges of trustworthy, resilient digital democracies through interdisciplinary collaboration.	C4DT, DIDAS
e-democracy, e-topia Part 2 Tags: Global, Digital assets, Digital signatures, Democracy, eGovernment	Olga Baranova, Laetitia Ramelet, Andrzej Nowak, Grégoire Barbey, Imad Aad, Katherine Loh	As democracies increasingly depend on digital services—like e-identities, e-voting, and e-collecting—new opportunities arise alongside risks such as fraud, privacy loss, and misinformation. The Center for Digital Trust (C4DT) at EPFL is seeking co-contributors for a session exploring the foundations and challenges of trustworthy, resilient digital democracies through interdisciplinary collaboration.	C4DT, DIDAS

Education Credentials and Digital Human Rights Tags: Global, Education, eGovernment	Open Discussion led by Kerri Lemoie (DCC), Kim Hamilton Duffy (DIF)	Discussion about the use cases for education credentials including micro-credentials, degree verification, and apostilles with an emphasis on interoperability and digital human rights -- safety, security, privacy	Ayra, DCC, DIF
Empowering Skilled People in Refugee/Displaced Context: Skilled Pathways pt 1 Tags: Global, Humanitarian	Darrell O'Donnell (Ayra), David Crawford (Fragomen/Ayra)	Leveraging skilled displaced people and refugees at a country level host: Ayra guests: states, international organizations, NGOs, and providers	ayra
Empowering Skilled People in Refugee/Displaced Context: Skilled Pathways pt 2 Tags: Global, Humanitarian	Darrell O'Donnell (Ayra), David Crawford (Fragomen/Ayra)	Leveraging skilled displaced people and refugees at a country level host: Ayra guests: country representatives	ayra
EUDI Wallet and payments: learnings from EWC and NOBID pilots Tags: Europe, Payments	Marie Austenaa (EWC), Thomas Kostka & Chiara Morresi (NOBID)	EWC and NOBID Consortium have jointly developed specifications and ran pilots in production. In this session you will learn: · How EUDI Wallets can be used for online payment SCA ensuring regulatory compliance with eIDAS2 and PSD2/PSR, · What are the learnings from EWC's pilot and what is required for further adoption? · How EUDI Wallets can unleash value by combining identity and payment credentials to enable innovative eCommerce checkout solutions · Beyond payment authentication, what are the opportunities for EUDI Wallets in payment and banking	LSPs
FIDO's Roadmap for Digital Credentials (Standards Track) Tags: Global	Andrew Shikiar, Lee Campbell, Tim Cappalli	FIDO Alliance has a global set of industry and regulatory stakeholders who have scoped and driven adoption of passkeys to help eliminate the world's reliance on passwords. Wallets and digital credentials are an immediate adjacency that could benefit from FIDO's protocols (CTAP) as well as its proven certification program and expertise in driving UX and branding for foundational identity technologies. This session will educate attendees on FIDO's background and feature open discussion on how FIDO Alliance's members and programs can most effectively engage moving forward.	fido
First meeting of the DCI Standards Committee	Ramesh Narayanan (MOSIP), Anita Mittal (GIZ), Adam Cooper (WB), Gail Hodges (OpenID)	This session marks the inaugural meeting of the DCI Standards Committee, co-organised by MOSIP and GIZ. It will bring together key stakeholders to initiate structured discussions on standards alignment, coordination mechanisms, and priority-setting for the Digital Credentials Initiative. The session aims to establish a shared understanding of the committee's scope and launch its collaborative work on advancing interoperability and trust in digital credential ecosystems.	MOSIP
First Person Credentials and Trust in the Open Source Supply Chain Tags: Global	Drummond Reed, (The First Person Project, Trust Over IP), Hart Montgomery (LF Decentralized Trust/Linux Foundation), Darrell O'Donnell (Ayra), Daniela Barboa (Linux Foundation, LF Decentralized Trust)	Securing the open source software supply chain requires verifiable trust signals for both code and contributor identity. This session will explore business, policy, and technical approaches to establishing trust, including the use of decentralized identifiers (DIDs), verifiable credentials, zero-knowledge proofs (ZKPs) for privacy-preserving attestations. We will also discuss the governance and compliance needs of such systems. We'll examine real-world implementations—from the current Linux Kernel's contributor validation to emerging frameworks that integrate First Person Credentials and government-issued	OpenWallet Foundation, LF Decentralized Trust, Ayra

		digital IDs—focusing on how these tools can be applied within CI/CD pipelines and open source project governance.	
First Person Credentials: From Concept to Implementation Tags: Global, Humanitarian, Organizational credentials, Education, Democracy	Daniela Barbosa (LF Decentralized Trust), Drummond Reed (First Person Project), Darrell O'Donnell (Ayra Foundation), Kim Duffy, (DIF)	Proof of personhood is one of the hardest problems in digital identity yet absolutely needed in this new era of generative AI. The First Person Project is a collaboration between LF Decentralized Trust, Ayra, ToIP, DIF, OpenWallet Foundation, and other partners to provide a truly decentralized, open standard solution. This session will cover the basic architecture of First Person credentials, wallets, and agents; demos of the user experience; and a roadmap for bringing it all to market at scale	LF Decentralized Trust, OpenWallet Foundation, ayra
Global Wallet Platform Requirements Tags: Global	Carsten Rosche (Ministry of Digitalization and State Modernization/DE), Andreas Frey Sang (CH), Ajay Gupta (CA DMV), Chris Goh (Austroads), Armando José Manzueta Peña (DO), Siddarth Pandit/Rick Byers (Google), Dawid Wroblewski (Samsung), Ramesh Narayanan (MOSIP)	This session intends to collect and discuss requirements relevant to the implementation of wallets in a secure, privacy preserving, sustainable and interoperable manner, ranging from hardware requirements, such as biometric functions, crypto algorithms, and secure key storage, to requirements regarding OS and Browsers, such as supported interfaces (NFC), APIs, protocols, formats, and respective governance. Also, it should be a forum for platform vendors to share their plans with the community.	GlobalPlatform, OpenWallet Foundation
GlobalPlatform technologies for wallets	Gil Bernabeu (GlobalPlatform), Mike Bergmann (BSI), Victor Hsieh (Google)	GlobalPlatform has been collaborating with GSMA, ENISA and member states but also with wallet developers, EU Large Scale Pilots and smartphone manufacturers to create a new deployement solution to deployed EU-DI wallet in eSIM or eSE Importantly, SEs are already standardized by GlobalPlatform and certified to stringent functional and security requirements. They provide a route to market via a widely-adopted technology and with minimal risk, enabling convenient and secure EUDI implementations that also support offline mode use cases when there is no active network connection.	GlobalPlatform
Governance in digital trade – Decentralization as response to challenges in a multi-polar world Tags: Global, Payments, Trade	Stephan Wolf, Phillippe Page, Scott Perry, Chandra Challagonda, Vijayakumar Manjunatha (Vijay)	The world is changing rapidly, placing supply chains and finance under increasing pressure. In a multi-polar world shaped by tariffs and transformative AI technologies, flexibility and speed are essential. Digitalisation and open networks offer a clear path to global market participation. Yet, governance remains a largely overlooked issue. Should we adopt the centralised frameworks of digital platforms, wait for regulatory direction, or explore more decentralised models that empower trading partners to choose their own governance approach? This session will explore the current landscape from legal, corporate, and IT perspectives—bridging public and private law.	Verifiable.Trade
hTrust — A Government-Grade Trust Registry That Serves 40 Million Citizens Tags: Asia & Oceania, eGovernment, Democracy	Ace Shim (Hopae)	hTrust is a government-ready trust registry based on a public, permission blockchain that is scalable, secure, and simple to operate. It powers verifiable public profiles of issuers, holders, and verifiers, and supports a tamper-proof revocation registry — all while remaining open, interoperable, and citizen-serving. This session presents hTrust's real-world impact at population scale, and how governments can bootstrap decentralized identity ecosystems without losing oversight.	OpenWallet Foundation, UNICC
Identity Foundations for Business Ecosystem Transformation and Industry 4.0	Dr. Juan Caballero (DIF), Dr. Susanne Guth-Orlowski (4TheRecord), Michal Jarmolkowicz (Swiss Safe), André Röder (Kaprion), Steffen Schwalm (msg	Decentralized identity is transforming how industries manage trust, security, and compliance across digital ecosystems. Starting with DIDComm standards and IoT applications, this session explores real-world implementations across Industry 4.0, Digital Product Passports, critical infrastructure, and high-security enterprise environments. We'll examine macro-economic	DIF, OpenWallet Foundation

Tags: Global, Payments, Digital assets, Organizational credentials	GmbH), Dr. Carsten Stöcker (Spherity GmbH)	impacts, explore applications in energy systems and supply chains, and review concrete deployments including EBSI blockchain infrastructure and the TRACE4EU project with eIDAS integration.	
Identity Systems and Threats: a holistic view Tags: Global	Carolin Beer (ETH Zurich), Sheila Zingg (ETH Zurich), Patrick Schaller (ETH Zurich), Xenia Hofmeier (ETH Zurich)	Traditional digital identities (e.g., logins, SSO, wallet ids, public/secret key pairs) focus on authentication. However, as life increasingly moves online, digital identity systems which allow users to prove statements about themselves (e.g., that they have a specific nationality or that they are over 18) have gained relevance. While such systems can enable new use-cases, identifying and enforcing the correct guarantees is a complex task and must balance the requirements of several stakeholders with different, and at times conflicting, needs. At the same time, ensuring the security of the system is critical as vulnerabilities can have severe implications (e.g., impersonation or data loss), which can erode trust in the system. In the first part of our session, we argue why classical approaches to threat modeling are not sufficient. We give an overview of the different layers that need to be carefully composed to provide integral security of a digital identity system in its entirety. As part of this, we provide examples of allegedly secure components, where their combination results in an insecure system. For the second part, we want to initiate an open discussion on the threat model(s) and security requirements necessary to establish the trustworthiness of digital identity systems.	W3C, OpenID
In-Depth Session on Unlinkability - A Non-Negotiable Requirement / ZKPs for Credential Presentation Tags: Global	Abhi Shelat (Google), Antoine Dumanois (Orange), Hart Montgomery (LFDT) René Mayrhofer (JKU), Christian Bormann (SPRIND)	Risks of issuer-RP collusion; where unlinkability is essential for public infrastructure (e.g., transport, location tracking). path towards globally accepted standards - what are realistic timelines to deploy the different options or how do we get towards somewhat realistic timelines? Discuss general requirements (like unlinkability) and technical options	LF Decentralized Trust, OpenWallet Foundation, DIDAS
Inclusive credential presentation - offline and low tech environments (Standards Track) Tags: Global	Sasikumar Ganesan	Presentation on the spec and next steps for a BLE based presentation using OpenID4VP protocol.	MOSIP, OpenID
International Trade: Identity across borders - combining SSI and authoritative registers Tags: Trade, Organizational credentials, eGovernment	Steve Capell (UN/CEFAT), Alina Nica Gales (registaroes.org), Drummond Reed (Ayra), Jose Cantera (IOTA Foundation), Jeanne Huang (UN/CEFACT)	High integrity digital identity is a foundational capability for international trade. Whether for customs authorities to reduce illicit trade, or for financial institutions to improve access to trade fiance, or to increase confidence in sustainabilty claims. This session will discuss the synergies between self-soverign identities such as W3C DIDs and authoritative identities such as maintained by national business and trademark registers. These are not competing alternatives but rather partners that can add value to each other.	UNECE, Ayra, IOTA Foundation
International Trade: Improving Compliance and Facilitation with Verifiable Credentials Tags: Global, Trade	Steve Capell, Sin Yong Loh (UN/CEFACT), Stephan Wolf (Verifiable.trade), Emily Benett (UNICC)	International trade processes are swamped with documents, many of which stubbornly resist digitalisation. This includes trade documents like orders & invoices, transport documents such as house/master air/sea waybills, finance documents such as letters of credit & cargo insurance, and regulatory documents such as import/export declarations & preferential certificates of origin. This panel examines the role of verifiable credentials as highly scalable and secure way to digitalise trade. Use cases will show how trade documents as verifiable credentials can reduce illicit trade, improve access to trade finance, and facilitate	UNECE, Verifiable.Trade UNICC

		legitimate trade. The panel will also discuss the challenges in digitalisation of a special class of "transferrable" documents such as ocean bills of lading.	
International Trade: Traceability and Transparency for the sustainable transition Tags: Global, Trade, eGovernment	Zachary Zeus (UN/CEFACT), Susanne Guth Orlowski (GBA), Beatrice Fernandez (UNEP), Brett Hylad (UN/CEFACT)	Supply chains play a pivotal role in the global transition to more sustainable production that reduces emissions, improves biodiversity, minimises forced labour, and increases re-use and recycling. Governments around the world are mandating climate related financial disclosures that require companies to measure their scope-3 emissions (i.e. emissions embedded in the upstream material inputs). Some regulators are also demanding product level disclosures such as the EU Digital product passport. The regulations as well as corporate social responsibility drivers are increasing the demand for more traceability and transparency in value-chains so that buyers at every step can make more informed decisions to choose more sustainable supply. As market access and/or price incentives propagate through the value chain, so the financial incentives to "greenwash" (i.e. make false claims about sustainability performance) will also increase. Digitally verifiable identities and sustainability evidence will therefore play a critical role in maintaining a level playing field and maintaining the value of more sustainable practices. This panel will discuss the challenges and solutions for supply chain traceability and transparency at a scale that can have a meaningful impact on global sustainability outcomes.	UNECE, GBA, UNEP
Interop through DX - Building Identity That Actually Works Tags: Global	Puria Nafisi Azizi (dyne.org), Ivan Marin Santamaria (GLEIF)	Interoperability fails because most teams prioritize spec compliance over real-world usage. At Forkbomb, we treat Credimi as a lab for fixing this—proving that developer experience (DX) decides whether a standard thrives or becomes shelfware. We'll cover: - Why conformance tools must mirror how developers debug, not how standards read - How to design flows that are testable, reproducible, and fail visibly - A blunt checklist for avoiding interop traps in wallets, issuers, and verifiers No jargon. Just lessons from building systems people actually use.	W3C, GLEIF
Interoperability for Digital Identity Solutions: Ensuring trust through testing Tags: Global, Drivers licence, Digital signatures, Digital travel, Payments, Car keys, eGovernment	Pieter Van der Honing (GlobalPlatform), Chris Goh (Austroads), Joseph Heenan (OpenID foundation), Mike McCaskill (AAMVA), Steve Pannifer (FIME),	In this session, we will explore the crucial aspects of achieving global interoperability for digital identity solutions to ensure digital identity a success globally. Key questions will include: 1. Why do we need technical interoperability in the first place? What are the challenges when it comes to interoperability? 2. What is current state of the market in terms of regulations, guidelines and methodology for interoperability testing? 3.How can we establish governance mechanisms, testing methods and tools against international standards and protocols that enable seamless integration and recognition of digital identities across different countries and platforms? 4. What steps need to be taken to ensure that, for example, an mDL issued in the USA is recognized and accepted in various scenarios worldwide, such as in alcohol retail stores?	GlobalPlatform
Investing in the Smart Data Economy	Irene Ng (Innoversa), Davide Ceper (Dataswyft), Tanya Troshyna (Affinidi), Thomas	The session will explore critical investment considerations across the digital trust infrastructure stack, from foundational protocols to consumer-facing applications.	LF Decentralized Trust, DIDAS, GLEIF, ayra

Tags: Global	Mayfield (Cardano), Ivan Mortimer (GLEIF), Nicholas Racz (KSC)	Participants will examine real-world adoption patterns, regulatory implications, and the evolving business models that are driving market transformation in identity verification, data sovereignty, and interoperable credential systems.	
Mapping Global Use Cases: Where ZKs (or other PETs) Are Essential Tags: Global, Digital signatures, Digital travel, Drivers licence, Health, Education, Payments, Organizational credentials, eGovernment	René Mayrhofer (JKU), Ying Tong (Ethereum), Daniel Saeuberli (DIDAS), Abhi Shelat (Google), Denis "Jaromil" Roio (Dyne.org Foundation)	Interactive session mapping privacy requirements across EUDI and trust ecosystems, defining zones where PETs are default.	DIDAS, OpenWallet Foundation, DIF
mDL Deep Dive (Session 1) Mobile Driver Licences Global Showcases from Issuers across Continents and Global OEM Wallet Providers Tags: Asia & Oceania, Europe, Global, North America, Digital travel, Drivers licence, eGovernment	Alan Stapelberg (Google), David Brudnicki (Apple), Florent Tournois (France Titres/France IDentité), Michael McCaskill (VP AAMVA), Christopher Goh (National Harmonisation Lead)	Driving licenses are used across jurisdictional borders and world-wide. The mDL ecosystem was designed to support this reality. Actual implementations that are being rolled out are illustrating international interoperability. This session will demonstrate this interoperability, share lessons learned so far in establishing the ecosystem, touch on remaining challenges, and explain how potential relying parties can consume mDLs.	ISO, mDL, AAMVA
mDL Deep Dive: Live Demonstrations of how mDLs are being verified globally from major events, airports, service centres and more. Tags: Asia & Oceania, Europe, North America, Global, Digital travel, Drivers licence, eGovernment	Michael McCaskill (AAMVA), Sebastien Bahloul (Idemia), Jess Dyer (FAST), Yash Shah (Credence), Oliver Tebu (MATTR), Chris Goh (Austroads)	Driving licenses are used across jurisdictional borders and world-wide. The mDL ecosystem was designed to support this reality. Actual implementations that are being rolled out are illustrating international interoperability. This session will showcase Global Interoperability across three continents with 4 relying party verifiers including banking terminals, stadium and event based systems and biometric verification systems for travel. EU, Australian and US production wallets and credentials will showcase realtime verification.	AAMVA, Austroads
mDL/mdoc in a nutshell (Standards Track) Tags: Global	Sebastien Bahloul, Oliver Terbu	mDLs have been a reality in the US accepted as an alternative to physical ID credential in TSA checkpoints starting in 2021 through Apple, Google and Samsung Wallet as well as DMVs apps (NY, CA ...). Generalized as mobile documents, this ISO standards' family has been also chosen by Australia and is also part of the EU Digital Identity Wallet ARF. Initially designed around in-person use case, it now supports remote/online presentment and will extend to provisioning, security, mobile document registry ... integrated with other Digital Identity standards (Digital Credential API, OpenID4VP, OpenID4VCI)	ISO
Meeting the Noncommunicable Disease (NCD) Challenge with Digital Wallets: Scaling Prevention and Person-Centered Care Tags: Africa, Asia & Oceania, Latin America & Caribbean, Global, Health	Jamie Guerra (WHO), Dr Douglas Bettcher (WHO), Hani Eskandar, (ITU), David Manset (ITU), Katja Rouru (Reach Digital) Panelist, Prof. Heung Youl Youm (Korea)	Noncommunicable diseases (NCDs) are the leading cause of death globally, accounting for over 70% of all deaths each year—many of them preventable. As countries pursue digital health transformation, interoperability and inclusion are key to ensuring that no one is left behind. Digital wallets offer a powerful tool to empower individuals with access to trusted, secure, and person-centred NCD prevention and care. This session will bring together experts from public health, technology, government, and implementation partners to showcase use cases where digital wallets and open source systems are improving NCD outcomes. The	ITU, WHO

		panel will highlight how Be He@lthy Be Mobile (BHBM) 2.0, a joint initiative by WHO and ITU, is expanding and to incorporate smart vouchers, digital credentials, and more — while building on global standards and locally relevant implementations.	
Open-Source Standards and Software as a foundation of European Digital Sovereignty Tags: Europe, Global	Paula Grzegorzewska, Torsten Lodderstedt (DE), Paolo de Rosa (EC), Herbert Leitold (AT), Vangelis Sakkopoulos (NiScy), Aleksandra (Ola) Ben Har (Google)	This panel will explore how open source standards and software can play a crucial role in strengthening European digital sovereignty by fostering transparency, innovation, and cooperation with the European digital ecosystem. A prime example is the European Digital Identity Wallet (EUDI) initiative, which leverages open source principles to provide citizens with a secure, privacy-respecting way to manage their digital identities, share documents and sign electronically. The discussion will focus on: The open development of the EUDI Wallet's technical specification, the Architecture and Reference Framework (ARF); The open development of the reference implementation of the EUDI including a mature solution and the necessary libraries; The active development and piloting of EUDI Wallets by the developer community; The valuable feedback and collaboration facilitated by a transparent development approach.	European Commission
Patterns + Problems + Solutions (Standards Track) Tags: Global, Organizational credentials, Digital signatures	Brent Zundel, Sean Bohan (OWF), Hart Montgomery (LFDT)	An extended version of the introductory session with an overview of the common patterns and problems that led to the development of digital credentials and the standards that exist as solutions.	IETF, OpenWallet Foundation, W3C
Piloting the EUDI Wallet: Educational and Social Security Credentials in Action Tags: Europe, Education, eGovernment	Lluís Alfons Ariño Martín, Gerd Bauer	The session will explore the implementation and piloting of educational and social security credentials within the European Digital Identity (EUDI) Wallet, as part of the EU-funded Large Scale Pilot project DC4EU. It will examine how trust models and governance frameworks are being developed to support the secure and verifiable issuance, exchange, and use of digital credentials—ranging from diplomas and professional qualifications to social security entitlements such as the European Health Insurance Card (EHIC) and the Portable Document A1 (PDA1). Presentations will address the regulatory and technical foundations provided by the revised eIDAS Regulation, practical challenges in cross-border verification, and real-world pilot scenarios. Speakers will demonstrate how these credentials can be integrated into trusted workflows using the EUDI Wallet, ensuring privacy, security, and interoperability. Live or simulated demonstrations will show how citizens can use the Wallet to access educational and Social Security services across borders, while public authorities maintain control and compliance. This session will offer valuable insights for policymakers, technical experts, and institutional stakeholders interested in the next generation of trusted digital identity in Europe.	LSPs
Powering Digital Sovereignty: Open Source, AI, and Global Standards for the Public Good Tags: Global	David Manset (BDT, ITU, and Digital Public Goods Alliance), Max Kintisch (DPGA), David Higgins (Digital Wallet Representative, GovStack)	As digital transformation accelerates worldwide, open source and open source AI are emerging as foundational pillars for inclusive, transparent, and sovereign digital ecosystems. This session explores how open source technologies and AI—guided by global standards such as the Digital Public Goods Standard and emerging open AI	ITU

		definitions—can drive innovation while ensuring trust, equity, and interoperability. Through concrete examples from multilateral and national initiatives, we'll highlight the strategic role of open ecosystems in shaping resilient digital infrastructures, fostering collaboration, and aligning with the Sustainable Development Goals.	
Privacy-Enhancing Technology: Achieving Unlinkability & other privacy properties Tags: Global, Digital signatures	Lead: Christian, Christian Bormann (SPRIND), Matteo Frigo (Google), René Mayrhofer (JKU), Imad Aad (C4DT-EPFL)	This session provides a focused update on privacy-enhancing technologies (PETs) with a spotlight on unlinkability and zero-knowledge proofs (ZKPs) in digital identity systems. It explores emerging schemes such as BBS+, SD-JWT, and ZK-mDoc, and assesses their maturity, real-world applicability, and post-quantum readiness. Experts will present insights into cross-sector requirements, implementation trade-offs, and shared terminology to help align understanding across technical and policy domains.	DIDAS, C4DT, OpenWallet Foundation
Protecting the Wallet - How much security is enough? Tags: Global, Car keys, Digital travel, Drivers licence, Payments, eGovernment	Fabien Deboyser (GlobalPlatform), Felix Bleckmann (BSI) Marie Austenaa (Visa), David Zeuthen (Google), Sasikumar Ganesan (MOSIP), Herbert Leitold (A-SIT)	This session will bring together leading voices from the banking industry, digital identity providers (including passport and national ID authorities), and other key stakeholders to: Unpack today's paramount wallet security requirements. / Identify and analyze major emerging security trends. / Engage in a critical examination of current approaches and chart the optimal path forward	GlobalPlatform
Public-private wallets interworkings Tags: Global	Anthony CARMOY (France Titres), Kamil Bak (Samsung), Alan Stapelberg (Google)	As Member States develop sovereign wallets to ensure trust, security, and regulatory compliance, the private sector continues to drive innovation and user adoption in the digital identity space. This panel brings together public and private actors to explore how to achieve meaningful interworking between both approaches—supporting industry growth while upholding the principles of digital sovereignty.	
SD-JWT and SD-JWT VC deep dive (Standards Track) Tags: Global	Daniel Fett		IETF
Second meeting of the Global Working Group on Technology Deployment and Procurement of DPI and Services Tags: Global	Julia Clark, Warren Smith, Pramod Varma, Kanwaljit Singh	This Working Group brings together key stakeholders from development organizations, the private sector, academia, and governments—including those involved in the design, development, financing, and implementation of Digital Public Infrastructure (DPI) worldwide. Its core objective is to foster a shared understanding and consensus around technology-neutral guidance to help countries navigate the complexities and trade-offs involved in DPI deployment and procurement. This second meeting of the Working Group will build on the priorities identified during the inaugural session held in March. It will focus on advancing guidance in several critical areas: procurement strategies for technology-agnostic DPI solutions and mitigation of vendor lock-in; reference architectures for DPI; a framework for evaluating solution options; a knowledge base of case studies; and practical guidance for project managers across the DPI implementation lifecycle.	World Bank Group, ITU, CDPI
Security and Interoperability Standardization for Wallets Tags: Global, Digital assets, Digital signatures, Payments	Julien Bringer (ISO/TC 307/JWG 4, BGIN), Mitchell Traves (BGIN), Carole House (BGIN), Paolo Campegiani (ISO 23042), Shin'ichiro Matsuo (Moderator)	One-hour workshop at GDC 2025 uniting BGIN and ISO experts to present ISO 23042 (Reference architecture for blockchain-based decentralized identity systems) under development and forthcoming wallet-security related standards, showcase BGIN cybersecurity streams, and engage regulators, vendors, and researchers on implementing and managing secure, interoperable digital wallets.	ISO, BGIN

Setting the Bar: Health Wallet Standards, Testing & Compliance Tags: Global, Health	Grahame Grieve (HL7), Hani Eskandar, (ITU), Cyril Seck (African CDC), Chinemerem Eyetan (WHO), José Costa Teixeira (PATH), Carl Leitner (WHO)	A technical roundtable exploring essential standards, testing protocols, and compliance frameworks for digital health wallets. Discussion will focus on defining the necessary requirements ('the bar') for secure, interoperable, and trustworthy solutions.	ITU, WHO
Showcase and demonstration/explanation of the ITB (Interoperability Test Bed) and the experiences of this platform in the LSPs. Explaining why this is a great (open source) platform to support interoperability testing for wallet ecosystems.	Esther Makaay, Nikos Triantafyllou, Lal Chandran	Showcase and demonstration/explanation of the ITB (Interoperability Test Bed) and the experiences of this platform in the LSPs. Explaining why this is a great (open source) platform to support interoperability testing for wallet ecosystems.	LSPs
Skills-based Economy & First Person Credentials Tags: Global, Education, Humanitarian	Darrell O'Donnell (Ayra), Etan Bernstein (Velocity Network Foundation), Wesley Teter (UNESCO), Drummond Reed (First Person/Ayra), Sharon Leu (JFF), Stéphanie Winet (IOE), Joan Beets (KennedyFitch), Tanya Troshyna (Affinidi)	The labor market has become increasingly global: individuals are globally mobile. Employers hire talent all around the world. Students study abroad and digital education and training platforms are have learners across the globe. Skills, competencies and experiences have become the building blocks of the world of work. Yet data on individual skills is often analog, local, and not easily verified – causing incredible friction for both employers and employees. This session is focused on mapping the requirements to enable global skills-based mobility in a frictionless, verifiable, digital way.	Ayra, LF Decentralized Trust
Sovereign by design: Panel	Javier Valiño (Eclipse Foundation), Christoph Strnadl (Gaia-X), Rajiv Rajani (iShare), Etan Bernstein (Velocity Network Foundation)	This panel is used as a follow up on the previous ""Sovereign by design: Trust Framework session"". How to create trust in digital ecosystems? Why credentials are critical to achieve this? How can we navigate the different regulatory and geographical challenges?	Eclipse Foundation, Ayra
Sovereign by design: Regulatory Compliance and the Cyber Resilience Act Tags: Global, Europe	Juan Rico (Eclipse Foundation), Daniel Thompson-Yvetot (Tauri), Roman Zhukov (Red Hat)	:: Welcome and introduction: CRA and Open Source :: Manufacturing European Software :: From Manufacturer to Steward: Red Hat's Approach to CRA Readiness :: Q&A	Eclipse Foundation, DIF
Sovereign by design: Trust Frameworks	Christoph Strnadl (Gaia-X), Rajiv Rajani (iSHARE), Etan Bernstein (Velocity Network Foundation)	Join us exploring the way credentials are used as a cornerstone of Trust Frameworks for Dataspaces and Data Exchange activities. In this session, relevant actors on the arena will present their approaches to achieve trust in such a demanding ecosystem. Agenda: - Gaia-X Trust Framework - Your Data, You Decide - Elements of a global self-sovereign trust framework - Q&A	Eclipse Foundation, Ayra
Standardization around QR code for proximity use cases Tags: Global, Digital Assets	Sasikumar Ganesan (MOSIP), Priyank Trivedi (OORU), Ameya Bhagwat (Tech5), Nicolas Chalanset (France Titres)	At France Identité, we leverage the proximity device engagement QR code, originally designed for device engagement, to also carry encrypted identity data. This enables fast, secure offline transmission of sensitive data, accessible only to authorized verifiers via QR scan—faster than BLE.	MOSIP
Sustaining Multi-Stakeholder Collaboration on ZKP & PET Development /	Daniel Saeuberli (DIDAS), Daniel Goldscheider, (LFDT), Paolo De Rosa (EC), Carmen Hett (UNHCR), more ad-hoc.	Discuss structures for ongoing working groups, funding mechanisms, and governance to support PET ecosystem evolution.	OpenWallet Foundation, DIDAS, UNHCR, C4DT, ETSI,

Standardization / Acceptance Tags: Global, Humanitarian, Health, Digital travel, Education, Payments, Digital assets			European Commission, LF Decentralized Trust, ITU
Technical Deep Dive Global Interoperability for DTC's			
The business case for wallet ecosystems globally, combining different work on economics and monetisation (global perspective) Tags: Global, Digital signatures, Digital travel, Drivers licence, Health, Education, Payments, Trade, Organizational credentials, eGovernment	Jon Shamah (Global Trust Foundation) Esther Makaay (Signicat) Katryne Dow Meeco.me	Establishing a commercial basis to Digital Wallets for Business is one of the major challenges for the ecosystem. With many Wallets now being deployed across the globa understanding some of the common principles is critical for cross-jurisdiction operability. No matter how good the technology, or how smart the idea, without a commercial model to ensure that all the actors can benefit the Digital Identity Wallet will wither at the vine and remain territorial only. This session will hope to lay out some foundamentals and global practices so that the digital wallets can fulfil their potential for both governments and the private sector.	GTF, LSPs
The business case on wallet ecosystems, combining different work on economics and monetisation (European perspective) Tags: Europe, Digital signatures, Digital travel, Drivers licence, Health, Education, Payments, Trade, Organizational credentials, Digital assets, eGovernment	Esther Makaay (EWC), Jon Ølnes (Signicat), Luigi Castaldo (Namirial)	Establishing a commercial basis to Digital Wallets for Business is one of the major challenges for the ecosystem. With many Wallets now being deployed across the globa understanding some of the common principles is critical for cross-jurisdiction operability. No matter how good the technology, or how smart the idea, without a commercial model to ensure that all the actors can benefit the Digital Identity Wallet will wither at the vine and remain territorial only. This session will hope to lay out some foundamentals and global practices so that the digital wallets can fulfil their potential for both governments and the private sector.	LSPs, GTF
The European Business Wallets: Outcomes and Insights from the EWC Large Scale Pilots Tags: Global, Europe, Organizational credentials, eGovernment	Andriana Prentza (UPRC), David Magård (Bolagsverket), Lal Chandran (iGrant.io), Werner Folkendt (Bosch), Carsten Stoecker (Spherity), Paolo de Rosa (European Commission)	This session presents the outcomes of the EWC Large-Scale pilot project on how we defined the Business Wallet and the organizational identity, called Legal Person Identification Data (LPID), and how we piloted the Business Wallet in different business scenarios. Through experts' presentations and demonstrations, we highlight the learnings for the pilots and what is required for further adoption so that business wallets can enable companies to do business simply and digitally.	European Commission, LSPs
The Recipe for Digital Health Credentials: Technical Standards & Government Experiences for Digital Health Credentials Tags: Africa, Latin America & Caribbean, Europe, Global, Health	Andrew Kajeguka (East Africa Community Secretariat), Carlos Javier Nuñez Contreras (RACSEL), Konstantin Hyppönen (European Commission – DG CNECT), Jennifer A Nelson (IADB), Garrett Mehl (WHO), Osama El Hassan (Dubai Health Authority)	Explores the end-to-end journey of implementing interoperable digital health credentials. Technical experts discuss foundational standards, challenges, and gaps. Government representatives share real-world implementation successes, challenges, and lessons learned (e.g., Hajj Health Card, LACpass) for cross-border health record solutions.	European Commission, WHO
The Solid standard, wallet storage and AI agents Tags: Global	Geoff Pirie (Inrupt), Davi Ottenheimer (Inrupt)	Solid is a W3C set of protocols that allow users to control their data and privacy. Using Solid as wallet-attached storage enables users to store, control access to and share with consent all types of data, not only credentials. The richness of data available in Solid backed wallets pave the way to agents and AI models, assisting citizens in their	OpenWallet Foundation

		interactions in the digital agoras. Wallet infrastructures need to include, besides identities, trusted storage, trusted communication and trusted execution environments.	
Threat Modeling Digital Wallets Tags: Global	Simone Onofri (W3C), Tara Whalen (W3C), Amir Sharif (Fondazione Bruno Kessler)	In this practical and collaborative session with a serious game, we will explore the threats and initial principles for addressing user considerations for high-assurance or real-world identity credentials and their use on the Web.	W3C, OID
Trust in transition: Digital Wallets and Humanitarian Cooperation Tags: Global, Humanitarian, Payments	Juriann Lahr (IFRC), Volker Schimmer (UNHCR), Jonathan Campbell (WFP), Nelson Goncalves (IOM), Emrys Schoemaker (Caribou), Margie Cheesman (Kings College)	The humanitarian sector is undergoing significant change in the face of funding cuts and efficiency drives. This workshop will explore what greater integration amongst humantiarian organisations might look like, and what concrete areas of collaboration there are - for example around shared risk (trust) frameworks.	IFRC, UNHCR
Trust Management: Mission Critical for Global Interoperability (Standards Track)	Arno Fiedler, Alex Tweeddale, Oliver Terbu	Trust Management is one of the most fragmented parts of the digital identity technical stack. Yet, it is absolutely crucial that the different standards for establishing trust play nicely together. This session will explore the different standards within the market: including X.509 certificate chains (eIDAS Trusted lists, VICAL, RICAL); OpenID Federation and alternative approaches (Swiss eID, EBSI, Ayra and other decentralized trust chains). Through a technical breakdown, we'll dissect why there is a spectrum of approaches, and why different models are required to meet different requirements. Moving forward towards an interoperable future, it will be essential to bridge different approaches to ensure a seamless user experience for users moving between different trust contexts.	ISO, ETSI, DIF, W3C
Trust Services, the backbone of EUDI Wallet ecosystem Tags: Global, eGovernment, Digital signatures, Digital travel, Payments, Drivers licence, Health, Education, Organizational credentials	Viky Manaila (CSC), Arno Fiedler (ETSI), Paolo De Rosa (EC) Rob Brand, Netherlands Ministry of Economic Affairs and Climate Policy); Tolis Apladas (EC), Jon Olnes (Signicat)	Explores the complexities, challenges and gaps in trust services provisioning for the EUDI Wallet ecosystem. Discussing the readiness of the market for implementation and acceptance, especially on the public administration and regulated industries. Trust is build on four pillars: legal, technical, Audit, Trust List.	ETSI, CSC, European Commission
Understanding Cyber Norms and the Rules-Based Order: What Are The Stakeholders' Roles in Protecting Critical Infrastructure? Tags: Global	Serge Droz (Swiss FDFA), Roman Zhukov (RedHat), Imad Aad (C4DT-EPFL)	This session will see representatives from the public sector, private industry, and academia engage in a Socratic dialogue, reflecting on the role of cyber norms and the rules-based international order in protecting critical infrastructure. Although states have agreed on the norms for responsible behaviour in cyberspace, turning these commitments into practical outcomes remains challenging. First, states have limited means for implementing norms and confidence-building measures (CBMs), and the main burden therefore falls on the private sector, which operates the infrastructure. Furthermore, states often fail to act on their commitments, as evidenced by the numerous malicious cyber operations. This raises questions, particularly during armed conflicts, when stakeholders may suddenly become belligerents. The session will explore how different stakeholders interpret and apply these norms and consider whether current frameworks remain relevant and actionable in today's security landscape.	C4DT
Unlocking Seamless Mobile Experiences: Multipaz & Open Mobile Hub Power Digital Identity	David Zeuthen, Troy Kensinger (Google), Diego Zuluaga (Open Mobile Hub)	Multipaz: The goal of Multipaz is to be a complete and comprehensive set of digital identity resources including (but not limited to) libraries, frameworks, and mobile reference applications with the intent of providing these	OpenWallet Foundation, EWC

and Cross-Platform Interoperability Tags: Global, Organizational credentials, Digital signatures		free to anyone who wants to use them. By doing so, both private and public entities can easily fork Multipaz to build a standalone digital identity solution with little to no friction. Open Mobile Hub: Open Mobile Hub (OMH) simplifies mobile fragmentation via a unified API for Maps, Authentication, and Storage across Android (GMS/non-GMS), iOS, and cross-platform frameworks. Its modular design lets developers swap map providers, OAuth services, and cloud storage backends without changing core code, ensuring consistent functionality. By combining Multipaz's open-source digital identity capabilities with OMH's unified cross-platform service modules, developers gain the tools to build truly interoperable and secure mobile applications, eliminating fragmentation from credentials to core services. "	
Verifiable credential based trust propagation for decentralized identity (Standards Track) Tags: Global	Prof H. Youm (ITU-T SG 17)	Trust propagation is the principle by which new trust relationships can be derived from pre-existing trust relationships. In addition, it consists of DIS platform that consists of service functions and functional components for facilitating the trust propagation. It is necessary to define a trust propagation framework for decentralized identity systems and associated components, functions and procedures in the decentralized identity management system.	ITU
Verifiable ID Chains as the Bedrock for AI Governance Tags: Global, eGovernment	Sunu Engineer (iSPIRT), Gaurav Aggarwal (iSPIRT), Harshit Kacholia (iSPIRT), Arthur Barichard (Deputy Ambassador, Digital Affairs, France)	As Artificial Intelligence evolves into complex adaptive systems, establishing clear lines of responsibility is paramount. This session explores the critical need for robust AI liability chains and posits identity chains as crucial for this effort. We will delve into how within ID chains, such as Zero Knowledge Proofs and Verifiable Credentials (VCs), can provide auditable trails for AI components, data provenance, and operational behavior. We would discuss this through a specific use case of child safety and AI. This enables a new way for effective regulation for AI.	Ispirt
W3C Linked Web Storage (LWS) Tags: Global	Jesse Wright (Open Data Institute)	This session introduces the W3C Linked Web Storage (LWS) Working Group and invites stakeholders interested in Web Storage Wallets to help shape its emerging specification. Participants will learn about the technical foundations and goals of LWS—enabling user-centric web applications with decoupled storage, identity, and access control. Drawing from the Solid Project, now stewarded by the Open Data Institute, the session includes a presentation by ODI's Solid Project Lead Jesse Wright, interactive discussion on stakeholder needs, and guidance on how to engage in the standards process.	LF Decentralized Trust, DIF, W3C
Wallet governance for blockchain applications Tags: Global, Digital assets, Payments, Digital signatures	Mitchell Travers (BGIN), Carole House (BGIN), Shin'ichiro Matsuo (BGIN)	One-hour workshop sharing the BGIN study report by the IKP working group, a systematic analysis of wallet governance across the full spectrum of financial, identity, and governance applications, providing critical frameworks for security, privacy, and regulatory compliance that the rapidly evolving digital wallet ecosystem urgently needs.	BGIN, OpenWallet Foundation
Wallets and a Wallet Ecosystem as a DPI Tags: Latin America & Caribbean, North America, Asia & Oceania, Europe, Africa, Global	Ajay Gupta (California), Chris Goh (Australia), Barada Prasad Sabut (India), Armando Manzueta (Dominican Republic), Ramesh Narayanan (MOSIP), Torsten Lodderstedt (Germany)	This session is intended to have presentations and a discussion on how wallet ecosystems can be introduced as a DPI, benefits, challenges, sustainable funding, public/private role play - EUDIW ecosystem in DE - CA DMV (US) - Austroads (AU) - Dominican Republic (DO)	MOSIP, AAMVA, OpenWallet Foundation, Austroads

What would it take for global acceptance of the W3C's Digital Credentials API? Tags: Global	Simone Onofri (W3C), Heather Flanagan (Spherical Cow Consulting)	The W3C Digital Credentials API will provide first-class Web browser support to mediate presentation and issuance of digital credentials. This session will encourage discussion about the API, its benefits, and blockers to adoption	W3C, OpenID
What's new in W3C Verifiable Credentials? Tags: Global	Pierre-Antoine Champin (W3C/Inria), Brent Zundel (Tradeverifyd)	W3C recently released a new family of specifications for Verifiable Credentials 2.0, making expression, exchange, and verification of digital credentials easier and more secure	W3C
World Bank Group with partners: Data and ID Wallets for MSME Finance: Enabling Verifiable Business Data Sharing and Capital Market Participation Tags: Europe, Trade	Ivan Mortimer-Schutts (GLEIF), Margrit Nzuki (IFC), Goran Vranic (World Bank Group)	Presentation of use case for application of digital organisation identity and verifiable data to the origination of invoice finance and factoring assets; the aim is to discuss prototype designs for enabling decentralized verification of data attributes and checks in the due diligence and risk assessment of financial assets for SME finance	GLEIF, World Bank Group
ZKProofs: From Crypto Potential to Regulatory Acceptance Tags: Global	Sebastian (ETSI), Luis Brandão (NIST), Abhi Shelat (Google)	Technical comparison of ZKP schemes (BBS+, ZK-mDoc); assess mobile readiness, interoperability, privacy assurances.	ETSI

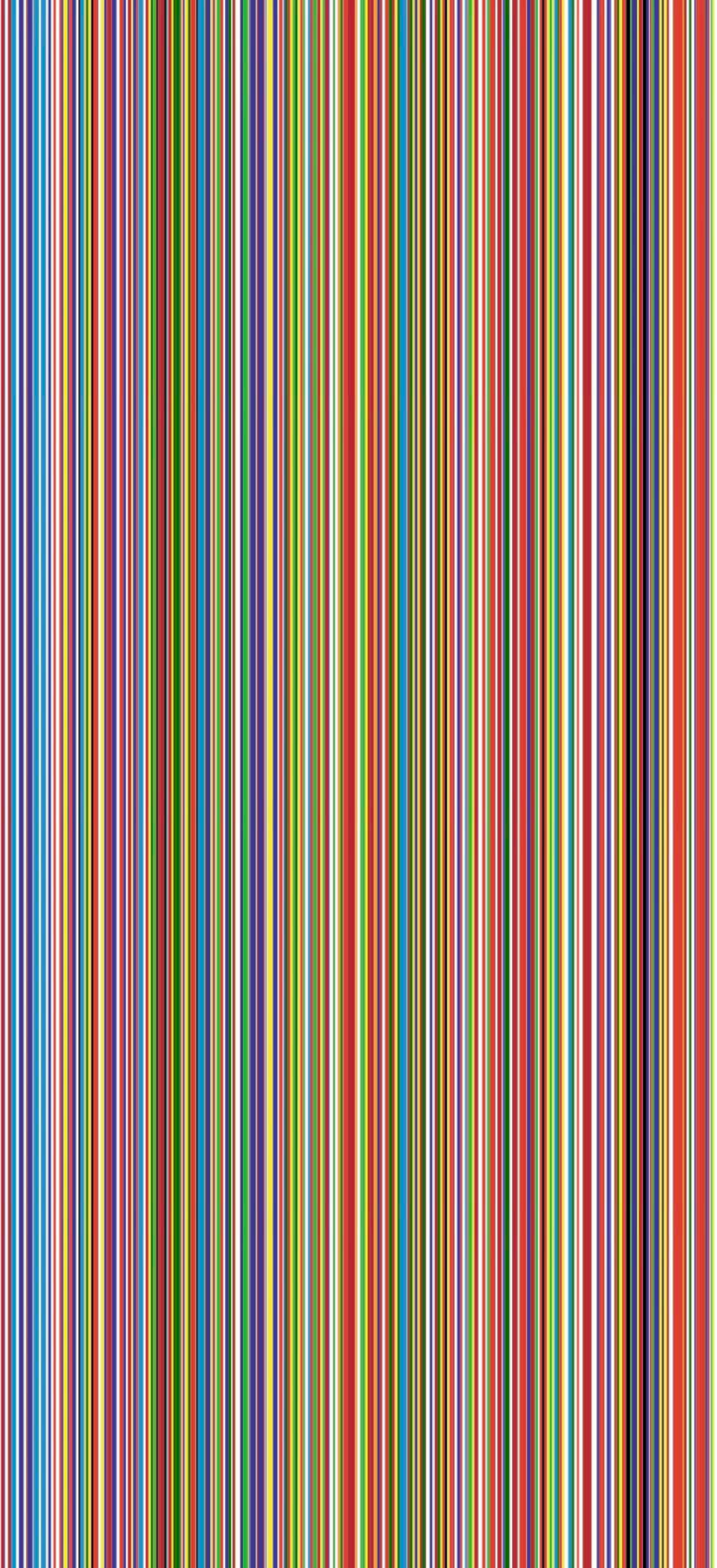
Imprint

Host of GDC25: Swiss Confederation; represented by the Federal Office of Justice FOJ.

Photography: Selina Reist, Federal Office of Information Technology, Systems and Telecommunication FOITT

Compilation of Book of Proceeding GDC25: Viola Bhattarai, Community & Ecosystem Consultant

For all inquiries, please contact: info@globaldigitalcollaboration.org



See you next time
September 1-3, 2026