BLOCKSTAND

Trust Models for Digital Identity

State of play

Author: Samuel Gómez (Gataca Labs S.L.U.)

Date: 10-04-2025

Version: 1.0

Table of Contents

Introduction

Digital identity systems rely on **trust models** to enable secure and trustworthy interactions among participants. As society moves services online, establishing confidence in digital identities has become a cornerstone for e-government, finance, healthcare, and beyond. This report provides an in-depth study of trust models for digital identity, with a primary focus on European frameworks and a comparative look at approaches in other regions (United States, China, Latin America, and others). It is written for policymakers, industry leaders, and identity professionals, adopting a formal yet accessible style. We will clarify what trust models and trust frameworks are, examine Europe's evolution from **eIDAS 1.0** to **eIDAS 2.0** (including the new European Digital Identity Wallet), compare global trust models, discuss business and governance considerations (including standards and pilot initiatives like EBSI and OIDF), and explore key challenges and future trends (interoperability, governance, privacy, standards like ISO 23042, blockchain-based self-sovereign identity, etc.). Throughout, emphasis is placed on real-world implications and the need for robust governance in deploying digital identity at scale. Figures and examples are included to illustrate concepts.

Definition and Role of Trust Models

Trust models define how confidence is established among entities in a digital identity system. In simple terms, a trust model lays out **how issuers, holders, and verifiers rely on each other's credentials and claims**. It specifies the technical and procedural mechanisms by which one party can trust that another party's digital identity assertions are valid and authentic . For example, a trust model might describe whether verifiers trust issuers directly or via an intermediary, how credentials are verified (cryptographic proofs, certificates, etc.), and what assumptions each role makes about the others.

Trust models are often illustrated by the classic **Issuer-Holder-Verifier relationship** – sometimes called the “trust triangle.” In this model, **the holder of credentials mediates between an issuer and a verifier**. The issuer and holder trust each other (the issuer provides a credential to the holder), the holder trusts the verifier (choosing to present credentials), and crucially the verifier trusts the issuer as the authoritative source of the credential . In decentralized identity systems, this triangle of trust is the fundamental paradigm (the verifier checks the issuer’s digital signature on a credential to confirm its validity) .

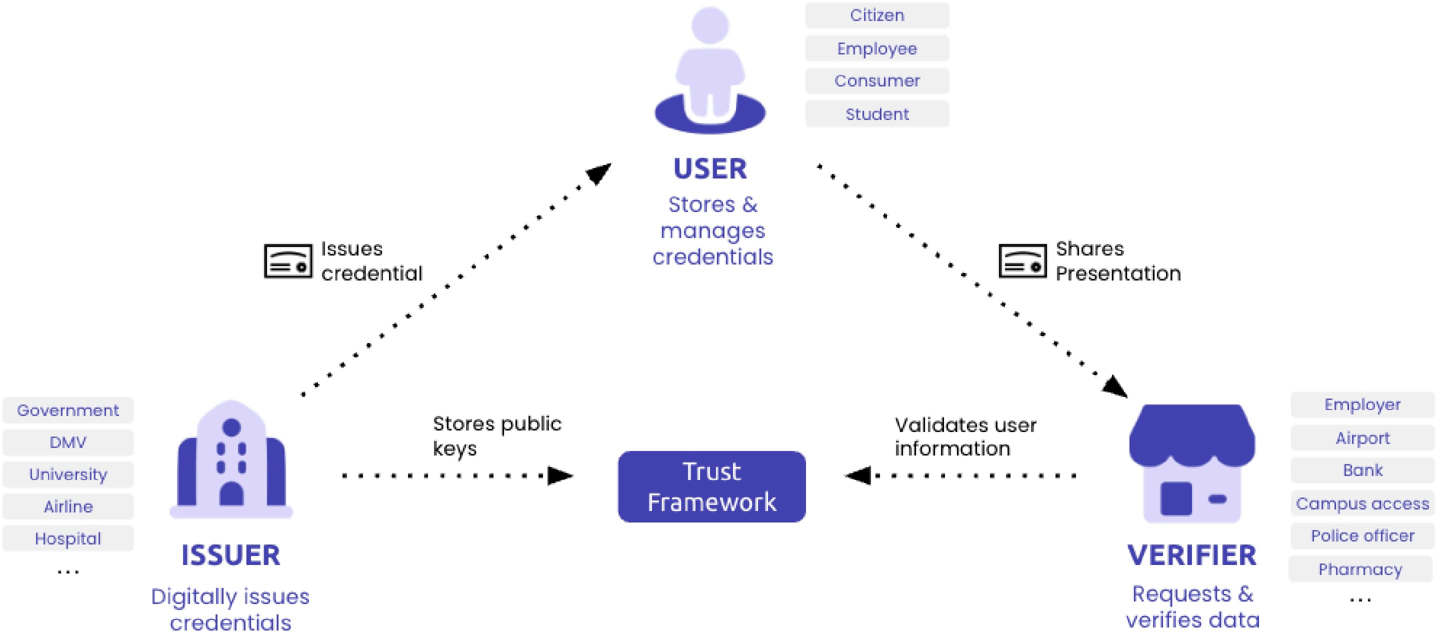


Figure 1

*Figure 1: The “triangle of trust” in a digital identity system (based on the W3C Verifiable Credentials model). An **Issuer** (left) issues a credential (e.g. a digital attestation) to a **Holder** (center) who stores it in a wallet. The holder later presents proof of this credential to a **Verifier** (right). A **verifiable data registry** (bottom, e.g. a blockchain or trust list) may be used by the issuer to publish verification material (public keys, status*

lists) that the verifier can check. This trust model ensures the verifier can trust the issuer's credential without the issuer and verifier needing a direct relationship.

It is important to distinguish **trust models** from **trust frameworks**. A *trust model* is a conceptual and technical design – "it defines how entities establish, manage, and verify trust relationships" in an identity system . In contrast, a **trust framework** is an overarching set of governance rules, policies, standards, and agreements that operationalize a trust model in a real-world ecosystem . **Trust frameworks** are essentially the **"rules of engagement"** that multiple organizations agree to follow to mutually accept digital identities . They typically specify requirements for identity proofing, credential issuance, authentication, security, privacy protection, and legal liability so that each participant can trust others' processes. For example, a government might publish a trust framework that identity providers must adhere to (through certification) in order for their digital IDs to be accepted for public services. As one industry definition puts it: *"A trust framework is a common set of standards-based rules that ensure minimum requirements are met for security, privacy, identity management, and interoperability through accreditation and governance"* . In other words, if the trust model is the **architecture** of who trusts whom and how, the trust framework is the **rulebook and infrastructure** that makes that trust operational and enforceable across organizations and jurisdictions.

Both trust models and trust frameworks play complementary roles in digital identity systems. The trust model provides the **technical basis** (e.g., whether trust is centralized, federated, or decentralized; whether the verifier checks a central authority or a blockchain for credential validation, etc.), while the trust framework provides the **business, legal, and policy basis** (e.g., contracts between identity providers and service providers, regulatory recognition of a credential type, liability rules). Together, they establish trust between the key roles in any digital identity transaction: the **Issuer** (entity that issues credentials, such as a government or bank), the **Holder** (individual or organization that possesses and controls the credential, typically via a digital wallet), and the **Verifier** (entity that needs to validate a holder's identity or attributes, such as a service provider) . The ultimate goal is that a verifier can confidently rely on credentials from a variety of issuers, often without having to integrate separately with each one – a feat achieved by agreeing on common standards and trust frameworks. For instance, in the W3C Verifiable Credentials trust model, verifiers decide whether they trust a given issuer (either *directly* or by checking if the issuer is accredited or on a trusted list) and then use cryptography to verify that any presented credential was indeed issued by that trusted issuer . This enables a more flexible trust model than traditional siloed systems, but it also requires governance: trust frameworks or registries may be used to help verifiers determine which issuers are trustworthy in the first place.

In summary, **trust models define the architecture of trust in an identity system, while trust frameworks provide the governance regime that makes that trust usable across organizations**. Both are critical: a robust trust model ensures security and technical integrity (e.g., preventing impersonation or forgery), and a robust trust framework ensures **mutual recognition and legal confidence** (e.g., that a digital driver's license or passport issued in one place will be accepted in another). In the next section, we examine how these concepts have been implemented in Europe, starting with the eIDAS Regulation's trust model.

European Trust Models

eIDAS 1.0: Centralized Trust via Qualified Trust Service Providers

The European Union's **eIDAS Regulation (EU 910/2014)**, adopted in 2014, established a groundbreaking cross-border framework for electronic identification and trust services. Under what we can call "eIDAS 1.0," the trust model in Europe was relatively **centralized and hierarchical**. Member States notified national eID schemes, and certain private providers could become authorized identity or trust service providers, but all within a tightly regulated trust framework. A hallmark of eIDAS's approach was the use of **Qualified Trust Service Providers (QTSPs)** as officially recognized issuers of trusted services like electronic signatures, seals, timestamps, and even (indirectly) identities .

Under eIDAS 1.0, each EU Member State could **"notify" one or more electronic identification schemes**, typically the government-issued electronic ID card or digital ID credential for that country. Once a scheme was notified and meets eIDAS assurance requirements, it must be recognized by other Member States' public services (this created a federated trust across Europe's public sector identities). In practice, most of these eID schemes were **government-operated or supervised**, meaning the trust model still rested on governmental authorities verifying and vouching for identity data. The trust relationships were managed centrally: each country's authorities trusted the others' notified eIDs because of the legal framework, and technical interoperability was achieved through standards and the EU's interoperability nodes.

For **trust services**, eIDAS established an even more explicit hierarchical trust model. A **Qualified Trust Service Provider** is defined as an entity accredited to issue qualified certificates or provide qualified electronic signatures/seals and other services with legal effect . Becoming a QTSP requires undergoing audits and a conformity assessment by a supervisory body . Each Member State maintains a **Trusted List** of its nationally supervised trust service providers (both qualified and non-qualified), and the European Commission provides a List of Trusted Lists (LOTL) to aggregate these. This effectively creates a **chain of trust**: if a digital certificate or signature is issued by a provider on an EU trusted list, it is recognized across all Member States as per eIDAS. In other words, Europe's approach was to **anchor trust in a set of certified authorities** – much like a governmental Public Key Infrastructure. Once an entity is a qualified provider, its credentials (certificates, signatures, etc.) are trusted everywhere in the EU internal market . This gave a high level of assurance and a **centralized trust anchor** (the regulatory regime and trust lists), which was necessary for cross-border legal recognition.

However, a centralized/hierarchical trust model has limitations. It can be less flexible in accommodating new kinds of credentials or private-sector issuers beyond those formally qualified. The eIDAS 1.0 model largely contemplated government-issued identities or qualified certificates as the means of electronic identification. It was less about user-controlled identity and more about *institution-controlled* identity (you authenticate against a national eID system, or you use a certificate issued by a QTSP). The advantage of this model is clarity and legal certainty – everyone trusts the "qualified" providers – but the drawback is potential lack of innovation and user-centricity, and the necessity of **bureaucratic processes for accreditation** which might slow down adoption. Indeed, by the late 2010s, the European Commission noted patchy usage of cross-border eID (few countries' eIDs were widely accepted across borders) and saw the need to update the framework for the next decade of digital identity.

eIDAS 2.0: Toward a Decentralized Trust Model

In 2021, the European Commission proposed a significant revision (informally dubbed **eIDAS 2.0**) to enhance the framework. Central to eIDAS 2.0 is the introduction of the **European Digital Identity (EUDI) Wallet**, which signals a shift to a more **decentralized trust model** for digital identity in Europe. Under eIDAS 2.0, every EU citizen and resident will be entitled to a digital identity wallet that can store a variety of **credentials issued by different parties**, not only a national ID . This is a move from the earlier centralized model (where typically a single national ID or a small set of providers were used) to a more **user-centric and multi-issuer ecosystem**.

In the eIDAS 2.0 trust model, **who are the issuers?** They include traditional authorities (e.g. national governments, population registries) *and* other entities that can provide "Electronic Attestations of Attributes." The regulation introduces **Electronic Attestations of Attributes (EAA)** as a new trust service category . Essentially, beyond issuing an eID for one's legal identity, issuers can also be organizations that attest to specific attributes – for example, a **university issuing a diploma credential**, a **bank issuing proof of a bank account or KYC status**, a **professional body issuing a license**, etc. Some of these attestations can be **"Qualified Electronic Attestations of Attributes (QEAA)"** if issued by a qualified trust service provider or an authorized public source. As such, under eIDAS 2.0, the circle of issuers expands: there still are government entities (for core ID information) but also potentially private entities that have authoritative data (educational degrees, financial identifiers, etc.), as long as they are accredited or recognized under the framework.

What documents or credentials can they issue? The scope is broad – essentially *any credential that can serve to prove identity or entitlements*. The regulation and its guidance explicitly mention that the EUDI Wallet can hold personal identification data (like name, date of birth, national ID number), **driver's licenses, passports,**

professional qualifications, academic credentials, health credentials, and so forth. For example, a university could issue an **academic credential** into the Wallet; a government could issue an **electronic ID card or residence permit** into the Wallet; a hospital could issue a **health certificate**. These credentials are **verifiable by design** (signed digitally) and, when qualified (QEAA), carry legal weight similar to traditional documents. Notably, the regulation mandates that **EAAs (even non-qualified ones) cannot be denied legal effect solely for being electronic**, signaling an intent that digital credentials become broadly accepted.

Who are the verifiers and what can they request? Verifiers are any public or private entities that need to check a user's identity or specific attributes. Under eIDAS 2.0, this could be a bank performing customer onboarding, an employer verifying a diploma, an airline verifying a traveler's identity, an e-government portal, etc. Verifiers can request **specific attributes or credentials** from a user's wallet – for instance, a verifier might ask for "proof of age over 18 and name" or "digital driving license" or "electronic health insurance card", depending on context. Importantly, eIDAS 2.0 emphasizes **data minimization and user control**: the wallet holder should be able to **choose what data to share** and only the necessary information for the given purpose . Large online platforms (e.g. social media or e-commerce above a certain size) will be **required to accept** the European Digital Identity Wallet for user authentication upon request, ensuring widespread utility. Crucially, the trust model means that the verifier does **not** need to call back to the issuer online for verification; instead, the verifier can check the credential's digital signature and validity (possibly consulting a **trusted registry or the issuer's public key**), so **issuers do not learn where/when the user is presenting credentials** . The user acts as the **"linking pin"** between issuer and verifier, without an intermediary tracking all transactions . This is a marked shift from earlier federated models where an identity provider might be in the loop for each authentication.

In summary, **eIDAS 2.0's trust model decentralizes some aspects of trust**. While it remains under a regulated umbrella (issuers of official credentials are still accredited or public bodies), the verification of credentials becomes more peer-to-peer (wallet to verifier) and multi-source. Users can accumulate credentials from various issuers in their wallet. Trust is no longer derived only from a single Identity Provider (IdP) per transaction, but from the cryptographic assurance of each credential and the governance that made that issuer trusted in the first place.

One way to describe this is that Europe is moving from a **"centralized identity provider"** model to a **"distributed credential"** model. In eIDAS 1.0, trust was often mediated by a central gateway (e.g., you log in with your country's eID system to access a service, the service trusts that eID system). In eIDAS 2.0, trust is mediated by the credentials themselves and the wallet: **the service provider (verifier) trusts the credential because it's signed by an issuer it recognizes as authoritative**, and because the wallet ensures it's presented with user consent. The issuer doesn't need to directly vouch for the user in real-time each time; it did so by issuing the credential. Verifiers are able to check the validity of a user's credentials without involving the issuers, since the user acts as the connecting element. This approach removes the need for any third -party intermediaries and preserves user privacy. This is essentially the self-sovereign identity (SSI) paradigm being integrated into a government-regulated context.

The European Digital Identity Wallet and Its Role

The **European Digital Identity Wallet (EUDI Wallet)** is the linchpin of eIDAS 2.0's decentralized trust model. The Wallet is a secure application (likely on the user's smartphone, though PC or cloud implementations are possible) that allows the user to **store credentials, manage them, and consent to sharing them** with verifiers . From a trust perspective, the wallet is where the **Holder** role is empowered: the individual has custody of their digital identity data and can decide whom to trust with it. This user-centric approach increases privacy and autonomy. Users no longer always rely on a central identity provider doing things behind the scenes; they actively **mediate the trust exchange** with cryptographically verifiable credentials.

The EUDI Wallet also brings some new trust framework elements: **Wallet providers** themselves will be certified/accredited to ensure the security and integrity of the wallet. In other words, while the contents of the wallet (credentials) are decentralized, the wallet software/hardware likely must meet standards (so that we can trust the wallet not to be easily hacked or spoofed). Each Member State is expected to “offer” a wallet to its citizens (or at least ensure one is available), but individuals can choose any compliant wallet. This means the trust model has an additional layer: verifiers and issuers must trust that a given wallet app is authentic and operated under the EU rules. eIDAS 2.0 anticipates this by creating a **“trust mark”** for compliant wallets and requiring mutual recognition of approved wallets . Thus, the governance expands to include **Wallet Providers** as another kind of actor in the ecosystem.

The significance of the EUDI Wallet in reshaping trust models cannot be overstated. It effectively **converts a previously federated system into a user-centric federated system**. The trust that was placed in member states’ eID systems is now extended to a broader set of credential issuers, and the user’s wallet orchestrates interactions. By 2030, the EU aims for a large majority of citizens to be using these wallets , with acceptance in both public and private sectors. This means businesses and governments across Europe will in practice be part of a **pan-European trust community**: if you trust the eIDAS framework, you will trust the credentials presented via the wallet, regardless of which country or sector issued them. The *types* of trust models that can be configured within this are also flexible. For example, Member States might maintain **trusted issuer registries** (to list which issuers are accredited for which credential types, possibly stored on a blockchain or other registry for verifiers to consult)

– indeed the European Blockchain Services Infrastructure (EBSI) is piloting exactly such a mechanism, as we discuss later. Alternatively, trust could be established via bilateral agreements or market-driven reputation in some cases, but the eIDAS regulatory umbrella means there is always a legal baseline of trust.

To sum up, **Europe's trust model is transitioning**: eIDAS 1.0's centralized, hierarchical trust (based on a few authorities and trust lists) is evolving under eIDAS 2.0 into a **distributed model** where many issuers can play, the user holds credentials, and trust is achieved through a combination of cryptographic verification and regulatory oversight of participants. Europe is essentially marrying the concept of **self-sovereign identity (SSI)** (which emphasizes user control and decentralized verification) with a **government trust framework** (to ensure security, privacy, and interoperability across the union). This hybrid approach could become a new paradigm for digital ID, influencing standards and implementations globally.

Global Trust Models Comparison

Trust models for digital identity vary widely around the world, reflecting different legal systems, cultural attitudes, and technological approaches. In this section, we compare Europe's approach with those in other regions – notably the **United States**, **China**, **Latin America** (with focus on Brazil and Mexico), and brief notes on other key regions (such as India and others). We will highlight who the common issuers are in each context, who the verifiers are, what credentials are used, and how trust is established or governed. Despite differences, many regions face common challenges of balancing security, privacy, and user convenience.

United States - Federated and Market-Driven Trust, with Emerging Decentralized Pilots

The United States lacks a single national digital ID system. Instead, its trust model for identity is a **patchwork of federated arrangements and private sector solutions**. Historically, identity in the US is often verified using physical documents (driver's licenses, social security numbers, passports) issued by different authorities. Online, the US has relied heavily on **federated identity** models in both government and industry.

In the public sector, the US government (federal level) established the **National Strategy for Trusted Identities in Cyberspace (NSTIC)** in 2011 to foster an "Identity Ecosystem" of interoperable identity solutions through public-private collaboration . The vision was to have multiple certified Identity Providers (IdPs) that individuals could choose from to authenticate to services, rather than each agency issuing its own credentials. While NSTIC did not fully achieve its lofty goals by the target dates, it did lead to the creation of login.gov, a single sign-on portal for U.S. federal agencies. login.gov itself is an example of a *federated model*: citizens create one account and can use it across many government sites, essentially making login.gov an **identity provider (issuer of authentication assertions)** that various federal agencies (verifiers relying on those assertions) trust. That trust is based on inter-agency agreements and NIST technical standards. Interestingly, even here, trust is not exclusive – some high-security agencies (like the IRS) opted to use a private-certified IdP (ID.me) for verification of users, due to perceived higher assurance needs . This illustrates the US approach: multiple credential service providers compete or coexist, and relying parties choose whom to trust (potentially requiring certain standards).

The role of **NIST (National Institute of Standards and Technology)** in the US trust landscape is primarily in setting **technical guidelines**. NIST's Digital Identity Guidelines provide a comprehensive framework for identity proofing, authentication, and federation.

They define **Identity Assurance Levels (IAL)** and **Authenticator Assurance Levels (AAL)**, as well as **Federation Assurance Levels (FAL)** to classify the strength of trust in a federated assertion. These guidelines serve as the basis for federal agencies and have influenced the private sector as well. For example, the US Government's Identity, Credential, and Access Management (ICAM) policies refer to NIST 800-63 for how to accept externally issued identities. The NIST guidelines also discuss **trust frameworks**: essentially recommending that agencies use providers who are accredited under some trust framework to meet those assurance levels . In practice, organizations like the **Kantara Initiative** ran trust framework certification programs where an Identity Provider could be certified as meeting NIST Level 2 or 3 requirements, etc. Thus, the trust model is **federated** (an RP trusts an IdP's assertion based on the fact that the IdP conforms to an agreed framework). The *legal* framework backing this is more ad-hoc: memoranda from the Office of Management and Budget (OMB) encourage cross-government federation , and contractual agreements are struck with commercial IdPs. There isn't a single law forcing all to accept one ID; rather, the government and industry converge by adopting common standards (like SAML or OpenID Connect protocols with agreed profiles).

For the **private sector in the US**, federation is prevalent in forms like the ubiquitous "Login with Google/Facebook/Apple" for consumer apps – here, tech companies act as **identity issuers (IdPs)** and other websites are verifiers (relying parties). Trust is established contractually and through technology: e.g., relying parties register with an IdP and trust its cryptographic tokens (JWTs, SAML assertions). There is no central authority approving Google or Facebook as IdPs; their trust comes from market position and the use of open standards. This *market-driven trust model* has worked for low-stakes authentication (convenience logins), but for high assurance identity verification (like opening a bank account), companies still usually have to perform their own KYC (know-your-customer) checks or use specialist identity verification services.

However, the US has been exploring **decentralized identity and verifiable credentials in pilot programs**. Notably, the Department of Homeland Security (DHS) through its Science & Technology Directorate has funded a **Silicon Valley Innovation Program (SVIP)** focused on **blockchain and digital credentials** for government applications. For example, DHS has supported projects to create digital, forgery-resistant credentials for immigration and citizenship documents, utilizing blockchain or distributed ledgers to verify issuer signatures . The goal is to prevent forgery of licenses and certificates by using **interoperable, decentralized verification**, rather than solely central databases . Several companies have worked on pilots such as a digital **driver's license** that could be verified offline via cryptographic proof, or a digital **work visa** that could be instantly validated for authenticity without querying a government database. These pilots often leverage the W3C Verifiable Credentials model, with issuers like state DMVs or DHS components, and verifiers like law enforcement or employers. While still experimental, they indicate a possible shift in the US trust model: trying to achieve **self-sovereign identity features under a voluntary, market-driven approach** (as opposed to Europe's top-down mandate).

Another development is at the state level: several US states (e.g., Arizona, Maryland) have started issuing **Mobile Driver's Licenses (mDLs)** – a digital version of driver's licenses following an ISO standard (ISO 18013-5). These mDLs can be presented via a smartphone app and verified by scanning a QR or via Bluetooth/NFC. The trust model for mDLs is somewhat decentralized: it uses **digital certificates issued by state authorities** embedded in the credential, so a verifier can trust the credential by verifying the state's signature. The federal government (**T**ransportation **S**ecurity **A**dministration) is running pilots accepting such mDLs at airports, setting the stage for cross-state acceptance. This again is a **distributed credential model** albeit within a specific domain (driving/ID).

In summary, the United States primarily uses a **federated trust model** supported by standards (NIST guidelines, industry protocols). Issuers range from government agencies (issuing documents or running IdPs like http://login.gov) to corporations (tech firms, banks, etc.), and there is pluralism – multiple competing identity providers. Trust frameworks (like Kantara, FICAM) have been used to raise confidence in certain providers for certain uses. **Verifiers (relying parties)** generally decide which providers or credentials to trust based on their risk tolerance, regulations, or customer convenience. For example, a bank might trust a credential that aligns with NIST IAL2 for remote account opening, whereas a social media site might accept a lower assurance login from Google. There is no single "wallet" or government-mandated digital ID, but the concept of **user-controlled identity data** is gaining ground through decentralized identity initiatives. The trust model in emerging pilots resembles Europe's SSI approach but without a unifying regulatory framework – instead it's happening via industry consortia and state collaborations. As one think-tank report noted, the US remains a "patchwork" of digital identity solutions, with efforts underway to create a more **nationwide strategy**. Legislative interest (e.g. the proposed "Improving Digital Identity Act") may eventually formalize cooperation, potentially designating trusted issuers of digital credentials (like state DMVs or federal agencies) that others can rely on. For now, the U.S. model exemplifies **bottom-up trust establishment**: it emphasizes interoperability and standards (technical trust), with governance often through contracts and market choices rather than central law.

China - State-Controlled Digital Identity

China's approach to digital identity is highly centralized under government control. The Chinese government has long enforced a strict **real-name registration regime** for both offline and online activities . Trust in identity is anchored to the national government’s identity infrastructure, and essentially the government (Ministry of Public Security and related agencies) is the ultimate **issuer and verifier** of identity information.

Every Chinese citizen is issued a **Resident Identity Card** (a physical card with a chip) that serves as the official personal ID. In the digital realm, China has extended this to what can be described as a **state digital identity platform**. For example, the government, through the Ministry of Public Security (MPS), has introduced systems like the “eID” digital certificate and, more recently, a proposed **“Network Identity” system** . The **Network Identity Authentication Public Service Platform** (proposal published in 2024) would issue citizens a **Network ID Number and Network ID Certificate** for use in online platforms . This effectively creates a government-run digital identity credential that online services can accept for real-name verification. Under this draft plan, individuals would apply through the national platform app, submitting their personal data (including biometrics like facial recognition) to obtain a Network ID . Once obtained, they can use that as a unified digital ID across internet services for login or account verification . The trust model is straightforward: **the state is the root of trust**. Any relying party (social media, e-commerce, etc.) that integrates with the platform will trust the Network ID certificate because it comes from the central authority. The user has little to no role in choosing issuers – there is essentially one issuer (the state), one credential (the Network ID), and many verifiers (all companies who must comply with real-name laws).

Even prior to this new initiative, major internet companies in China have been required to validate users’ identities against government databases. For instance, to register for a WeChat or Weibo account, users must provide their national ID number and sometimes a facial verification which is checked by the platform using governmental or telco data. Telecommunication providers require passport/ID uploads for mobile SIM cards. All of this amounts to an ecosystem where **the government identity (and**

associated biometrics) is the ultimate trust anchor, and private companies act as enforcing agents by integrating government ID checks into their onboarding processes .

China's trust framework is deeply entwined with national security and surveillance considerations. It is **highly hierarchical** – much like a classic PKI but controlled by state agencies. Recent moves suggest even tighter integration: an official **"digital identity card" (e-ID)** that can be loaded into popular apps. For example, pilot programs allowed residents to add a digital version of their national ID card into the **Alipay or WeChat app** as a form of official ID . These digital IDs are still issued and authenticated by the government; the tech platforms are just a user interface.

In terms of credentials, the primary one is the **citizen ID (Shenfenzheng)** data. But China is also rolling out a **Digital Social Security card**, **Digital Driving License**, and other such credentials within apps – again all issued by government departments. These are often available through the government's **"Internet+" platforms or the national mobile app for e-government.**

Verifiers in China are basically *every service provider*, because regulations mandate nearly all online services verify users. They either rely on the user's ID number (checked via an API to a government or telco database) or increasingly on the new unified digital ID services the government provides. The trust model is thus one of **complete state control and central verification**: if the government says an ID is valid, the verifier accepts it; if not, the person cannot access the service. For offline scenarios, police and authorities have devices to read the chip on the physical ID card to verify it, which is analogous to the online trust in the government's digital verification.

From a governance perspective, China's model ensures a single source of truth – which simplifies interoperability (no competing standards; everyone uses the national ID). However, it raises privacy and civil liberty concerns: the **same identifier gets used everywhere**, and the state can theoretically track all identity usages. Indeed, the system is designed to **combat anonymity**. The new Network ID proposal tries to address data protection superficially by saying it's voluntary and claims it won't track browsing, but given it links everything to a central platform, it effectively could enhance surveillance.

It's also worth noting that **biometrics** are heavily used in China's identity trust model. Trust is not only in "something you have" (ID number/card) but reinforced by facial recognition. For example, fintech apps performing real-name verification often prompt the user to do a face scan which is matched to the national photo database. This is a way to prevent impersonation – the trust model assumes *if the face matches the ID data from the government, then it's the true person*. The government has set up cloud services to enable such biometric ID checks for authorized businesses.

In summary, **China's digital identity trust model is centralized and state-driven**. The government is both the primary **Issuer** of identity (and all crucial attributes) and effectively an overseer of all **Verification** (since verifiers must use government-approved methods). Unlike Europe's emerging model or the US model, citizens in China do not control credentials or choose from multiple providers – they have an official digital identity that is universally required. This model achieves a high degree of trust among verifiers (because the government's word is final) and makes fraud difficult (it's hard to fake the national ID given the biometrics and secure chip). The downside is low user privacy and potential abuse of the centralized power.

Globally, China's model is being observed and, in some cases, emulated by other countries with similar governance philosophies. There is also an international aspect: China is reportedly working on mechanisms for **cross-border recognition** of its digital ID or integrating it with services like travel (for instance, their health code apps during COVID and plans to link national ID with travel records). But fundamentally, the trust model remains **hierarchical** – *"trust the government, which trusts no one else equally."*

Latin America – Federated and Emerging Approaches (Brazil and Mexico)

Latin American countries have diverse identity systems, but many are in the midst of digital transformation. Two of the largest countries, **Brazil** and **Mexico**, provide instructive examples of trust models that blend federated approaches with strong government oversight, albeit in different ways.

Brazil has historically had a fragmented identity system (each state could issue ID cards, plus a national taxpayer ID number, etc.), but recently it has made strides toward a unified digital identity. The Brazilian government's main digital identity initiative revolves around the GOV.BR **portal and account system**. The GOV.BR **Account** is a federated digital identity that allows Brazilians to access over 4,000 online services of the government with a single login . The trust model here is federated and multi-tiered: Brazil's GOV.BR accounts have three levels of assurance (Bronze, Silver, Gold) depending on how the user was verified (e.g., self-assertion vs. biometric verification against government databases, etc.) . Users can even choose **"sign in with bank credentials"** as a verification method – Brazil has an arrangement where major banks (which already KYC their customers) can serve as identity providers to bootstrap a GOV.BR account (this is analogous to the **"bring your own identity"** approach) . In fact, Gartner analyst Arthur Mickoleit highlighted Brazil's GOV.BR and France's FranceConnect as examples of governments connecting multiple IdPs under an umbrella scheme . In Brazil, a citizen can log into GOV.BR using their banking login via an integration; once in, that can upgrade their account assurance since the bank validated their identity. This indicates a **federated trust framework** where government services trust certain private issuers (banks) and other public issuers (the electoral bureau, etc.) through the GOV.BR federation.

Brazil also has a national public key infrastructure called **ICP-Brasil**, which issues digital certificates (for electronic signatures, etc.). Those certificates serve as high-assurance identity credentials (e.g., an **e-CPF** certificate binds to one's tax ID). The trust model there is classic hierarchical PKI, supervised by a governmental IT institute. Many Brazilians, however, do not have an ICP digital certificate (it's often used by professionals or companies). The more mass-used identity factor is the **CPF number** (a national ID number) which is now being incorporated into a new **National Civil Identification (ID Digital)** that unifies various docs. In 2022, Brazil launched the **CIN (Carteira de Identidade Nacional)** – a new national ID card with a QR code that links to the holder's biometric data on a central system . The **CIN can also be issued in digital form** via an app, and it uses the CPF as the unified identifier. So Brazil is moving to a model where the **federation is within its government**: multiple agencies contribute data (civil registry, biometric database) but result in one digital ID credential.

Thus, Brazil's trust model is partially federated (GOV.BR federating multiple IdPs including banks) and partially unified (one national digital ID card). We can characterize it as **"government-mediated federation"**. The issuers: Government agencies (federal tax authority issues CPF, federal police issue passports, state bodies issue driver's licenses, etc.), and also **banks as identity verifiers** in the digital login context. Verifiers: both government services and private relying parties. Indeed, Brazil explicitly aims to allow the GOV.BR **identity to be used for private sector services too**, effectively becoming a national digital ID platform. The trust frameworks involved include law (Brazil has a legal framework for digital signatures and is developing one for digital ID) and standards (they leverage FIDO for some authentication, and OAuth/OpenID Connect for GOV.BR SSO). A notable point: Brazil is connecting silos – e.g., by linking bank logins (already strong due to banking regulations) with government logins, they overcame adoption hurdles rapidly. By late 2024, GOV.BR **had over 100 million users**. This demonstrates how a federated trust model, if well-governed, can achieve scale.

Mexico, on the other hand, has had an identity landscape that is both centralized on paper and fragmented in practice. Mexico issues a national unique population registry code (CURP) to each citizen and resident, and most have a physical voting ID card issued by the electoral authority (INE) which acts as the de facto ID. But Mexico has not until recently had a universal digital ID system. The trust model has been that different agencies and private companies each verify identity via documents (e.g., banks use the INE card and CURP for KYC, often checking against government databases in the background). To streamline this, Mexico has been working on a **"Unique Digital Identity Card (CUID)"** – a project to create a mandatory biometric ID database and card . The proposal (as of 2021) was to compile all citizens' and residents' biometrics (fingerprints, iris, face) and data in a **central database**, and issue a digital ID credential tied to that . This is somewhat akin to India's Aadhaar model (discussed below) or an extended version of Mexico's existing CURP with biometrics. The trust model for the proposed CUID is **centralized**: the government (through RENAPO, the national population registry) would be the sole issuer of the digital ID, and all verifiers (banks, hospitals, etc.) would trust it by querying or validating against the national system. The project raised significant privacy concerns. As of the latest updates, full implementation has faced delays and criticism. However, Mexico has deployed some pieces: for instance, a **digital birth certificate** system, and a way to verify CURP online via government services.

In absence of a fully realized national digital ID, Mexico's current trust model for digital identity is somewhat **federated via databases** – different ministries have their own identity databases (e.g., the National Population Registry for CURP, the National Electoral Institute for voter ID data, etc.), and service providers often have to cross-check individuals against those. For example, when you sign up for a financial account, the bank might use a government API to verify your CURP and maybe check your ID card's authenticity. This is a weaker federation (not user-centric, but a patchwork of back-end checks). Mexico also does not have a single sign-on like GOV.BR or http://login.gov . Each agency has its own portal (some allow linking accounts via the CURP or tax ID).

One interesting initiative in Mexico is the use of the private sector for KYC: Mexican banks created a platform to share biometric validation results (to combat identity fraud among banks), which is a form of **industry federation** of identity proofing (the idea being if one bank has verified your identity and captured your biometrics, another bank could trust that via the shared platform, avoiding repeat onboarding friction). This is not nationwide yet, but it indicates movement toward federated trust within sectors.

So for **Mexico**, issuers are mainly government agencies (civil registry issuing CURP, INE issuing voter ID, etc.), and verifiers span government and private (banks, telcos, etc. all legally required to do identity verification). They are working toward a model where the **federal government becomes the one issuer of a unified digital ID (CUID)**, which would then be a single credential everyone trusts – **similar to China in centrality, but likely using modern tech like biometrics and perhaps mobile app integration**. Until that happens, the trust model remains a combination of manual document verification and siloed electronic checks.

Other Latin American countries often have either a single national ID number (sometimes with biometric cards) or are introducing digital ID wallets. For example, **Argentina** has the Mi Argentina app which holds a digital version of one's national ID and driver's license. **Peru** and **Chile** issue electronic ID cards with chips and are exploring mobile ID. Many have taken inspiration from **Spain's DNIe or Estonia's e-ID** in implementing smart IDs. The trust models vary from **strict government issuance** (like Argentina's government issues all digital credentials via its portal) to **public-private partnerships** (as seen in some banking federations or in **Chile id** which can use the national tax ID authentication or social media accounts depending on service).

Commonalities and Differences

- In **issuers**: Europe and Latin America put governments strongly in the issuer role (for foundational ID), whereas the US relies more on diverse issuers (including private). China exclusively uses government as issuer. Brazil and some others allow banks to serve as identity verifiers under a government umbrella (so quasi-issuers of credentials or assertions). India (discussed next) is like China in that government is issuer of a foundational ID (Aadhaar) but they let private e-KYC providers use that ID for verification.
- In **verifiers**: globally, verifiers include government services, financial institutions, employers, etc. The difference lies in how easy it is for a verifier to trust an external issuer. In EU, trust lists and eIDAS framework make it straightforward (any qualified issuer's credential must be accepted). In the US, each verifier decides which IDs to accept (leading to use of driver's license or SSN as defacto, but no universal acceptance of one digital ID). In China, verifiers effectively have no choice – they must integrate with the national system. Latin America is moving toward European-style frameworks (e.g., an Argentine business can trust the Mi Argentina credential as it's government-certified).
- In **credentials**: Traditional credentials like passports, national IDs, and driver's licenses are being digitized everywhere. Europe is adding novel credentials (like professional qualifications in wallets). The US has nascent digital driver's licenses and many private credentials (like an "ID.me verified veteran" credential, etc.). China's primary credential is a digital ID tied to biometrics. Latin America is focusing on digitizing national ID cards and linking them to mobile apps. Also, **biometrics** play a heavy role in many regions (India, China, increasingly LATAM) as a way to secure trust.
- In **trust establishment**: Europe uses legal mutual recognition and technical standards; the US uses standards and market-driven trust (with government guidelines but not one law); China uses law and centralized control; Latin America often uses law (e.g., Brazil's legal framework for CPFs and digital certs) combined with newer standards adoption.

One notable global trend is the influence of the **self-sovereign identity (SSI), ISO and W3C Verifiable Credentials model**. Europe explicitly uses it in eIDAS 2.0; the US pilots use it; countries like **Canada** (not covered in depth here) have a **Pan-Canadian Trust Framework** and have piloted SSI (e.g., digital government services in British Columbia using verifiable credentials). In the Middle East, countries like **Dubai (UAE)** launched a blockchain-based digital identity (UAE Pass) which is also a sort of federated wallet. **Australia** has a federal identity framework (myGovID) and a Trusted Digital Identity Framework (TDIF) that accredits multiple IdPs including potentially banks, similar to Canada and the UK's attempted Verify system. So globally, we see **convergence toward a few models**:

1. **Government-centric unified ID** (China, India, many developing nations) – high assurance, central trust.
2. **Federated public-private** (US, Canada, Brazil, EU in some aspects) – multiple issuers, trust via frameworks/agreements.
3. **User-centric decentralized** (EU Wallet, SSI pilots in various places) – credentials travel with user, trust via cryptography and governance registries.

A quick note on **India**, as it's one of the largest identity systems: **India's Aadhaar** is a digital identity for over 1.3 billion people, where a single government authority (UIDAI) issues a unique ID linked to fingerprints and iris scans . Aadhaar is used to authenticate identity for a vast array of services – banks, welfare distribution, telecom SIM registration, etc.

The trust model is centralized but with open APIs: any authorized service provider can use Aadhaar authentication (online fingerprint/iris or OTP verification through UIDAI) to trust a user's identity . Over **95% of Indians have Aadhaar** making it a near-universal credential. Yet India also layered a bit of user-centric approach: they offer an "offline KYC" where the user can download a digitally signed XML or QR code from UIDAI to share with a verifier without the verifier pinging the central database. This provides some privacy. India’s model thus is **central issuance (government ID) combined with both centralized and decentralized verification modes**. The success of Aadhaar (and its massive scale) has influenced thinking in many countries. For example, several African countries have implemented or are planning similar national biometric ID systems (e.g., Nigeria’s NIN, Kenya’s Huduma Namba, etc.), leaning on a **central trust** model to bootstrap digital services.

In conclusion, global approaches to digital identity trust can be seen along a spectrum: from **centralized state models (China, India)** to **fully decentralized user-controlled models (SSI in theory)**, with many **hybrid federated models (EU, US, Canada, Brazil)** in between. Each has trade-offs. Europe’s approach under eIDAS 2.0 is notable because it tries to combine the strengths of different models – legal assurance from a government-led framework with the flexibility of decentralized credential exchange. Other regions often emphasize one aspect: the US emphasizes market choice and innovation (at cost of coherence), China/India emphasize central authority (at cost of privacy), etc. These differences mean that international interoperability of digital IDs remains a challenge – a topic we will revisit when discussing future directions and standards.

Business and Governance Perspectives

From a business and governance point of view, trust models in digital identity have far-reaching implications. The success of any digital identity ecosystem depends not just on technology, but on **adoption by users and service providers**, compliance with regulations (privacy, security, sector-specific rules), and alignment with industry standards for interoperability. In this section, we discuss how various trust models impact business considerations: what are the **adoption barriers** and incentives? How do regulatory compliance and regional policies shape the trust models? What roles do industry groups and standards bodies (like the **OpenID Foundation** or others) play in fostering interoperability? We also examine specific governance initiatives such as the **European Blockchain Services Infrastructure (EBSI)** – which is piloting decentralized identity in a public-sector context – and how **hierarchical vs. decentralized trust structures** might coexist. The focus here is on a non-technical, organizational perspective: what do companies and governments need to do to make these trust models work in practice?

Adoption Barriers and Drivers

One of the biggest challenges in implementing any digital identity trust framework is achieving wide **adoption**. For a trust model to deliver value, a critical mass of **issuers, holders, and verifiers** must participate. Several barriers often stand in the way:

- **Lack of Mutual Recognition:** Service providers may be hesitant to accept identities or credentials issued by others unless there is a clear trust framework. In absence of a strong framework, **businesses fear liability** or fraud if they rely on an external identity. For example, before eIDAS, a bank in country A might not accept a digital ID from country B due to uncertainty. With eIDAS and its **common rules**, that barrier is lowered because a bank knows a notified eID from any EU country meets certain standards (LoA). This shows governance can drive adoption by building confidence . Conversely, in a fragmented environment like the US, a relying party often still asks for "government-issued photo ID" to be uploaded, rather than trusting a third-party digital credential, because there isn't an universally accepted trust framework in consumer space yet. Overcoming this requires either regulation or strong market signals.
- **User Experience and Trust:** Users need to trust the system to adopt it. If the trust model is too complex (e.g., requiring managing certificates or keys) or if users fear misuse of their data, adoption suffers. **Convenience is key** – this has driven popularity of social logins and, in countries like Brazil, the integration of bank logins into gov accounts (users find it easy, so they use it). Conversely, if a digital ID requires an in-person visit or cumbersome setup, users may not bother,

leaving the system underutilized. So, **businesses and governments must invest in user-friendly implementations** (mobile apps, biometric logins, etc.) and awareness campaigns to drive uptake.

- **Privacy and Data Protection Compliance:** Regulatory compliance, especially with privacy laws like Europe's GDPR, is a major factor. Trust models that involve centralized data raise compliance concerns (storing lots of personal data can be risky). Models that allow selective disclosure and user control (like SSI) are privacy-enhancing, which can make them more acceptable to both regulators and users. Policymakers in Europe explicitly designed the new trust model to be GDPR-aligned – the EUDI Wallet lets users share only specific attributes, minimizing data exposure . Businesses are attracted to models that reduce their **data liability** (for instance, verifying age via a yes/no credential instead of storing someone's full ID info). This compliance benefit can drive adoption from the business side because it means less risk and possibly easier regulatory audits. However, aligning a trust model with privacy laws can also impose design constraints (e.g., ensuring no unnecessary personal data flows through the system). Governance frameworks often bake in such requirements, as eIDAS 2.0 does by forbidding issuers from collecting extra data when the wallet is used .
- **Cross-Sector and Cross-Border Complexity:** For businesses operating internationally, dealing with many different trust models is challenging. If each country has its own digital ID solution, a global company must integrate with each (which is costly). This creates a barrier to adoption – companies might not bother except for the largest systems. Initiatives like eIDAS (which provides a single European framework) or the **OpenID Foundation's Identity Assurance framework** (providing a standard way to convey verified identity data via OpenID Connect) aim to solve this by standardization. The **OpenID Foundation (OIDF)**, a major industry body, plays a key role here. It develops and promotes open standards that can carry trust across domains – for example, **OpenID Connect** (OIDC) is widely used for federated login, and now OIDF has introduced profiles like **OpenID Connect for Identity Assurance (OIDC4IDA)** that allow an Identity Provider to include verified attributes (like passport info, etc.) in a standard token

. This profile was designed with eIDAS and other frameworks in mind, to bridge the gap between government-issued identity data and modern API-driven authentication. By adopting such standards, industry and governments can lower technical integration costs – a bank's system might accept an **OIDC token with verified attributes** from any compliant IdP, whether that IdP is Estonia's government eID or a commercial IdP that did KYC, as long as they trust the framework behind it.

On the flip side, there are also drivers for adoption:

- **Regulatory Mandates:** If a law requires acceptance of a certain digital ID (as eIDAS 2.0 will require large platforms to accept the EU Wallet), businesses have to comply, which accelerates adoption. Similarly, India mandated businesses accept Aadhaar eKYC in many sectors, driving rapid uptake.
- **Cost Savings and Efficiency:** Digital identity can drastically reduce onboarding costs, fraud losses, and transaction friction. A robust trust model lets businesses reuse identity verifications – e.g., a user who has a government-issued digital credential can open accounts faster, which means the business spends less on manual verification. Governments also save costs by not issuing paper documents or handling in-person verification if digital works. These economic incentives are strong – estimates of billions saved in customer onboarding and password recovery push companies to federated identity solutions.
- **Security Benefits (Fraud Reduction):** Strong trust models (like using cryptographically verifiable credentials, multi-factor auth, etc.) can reduce fraud. For instance, banks in the UK found that using the GOV.UK Verify (when it existed) or mobile identity verification could cut down identity theft compared to relying on scanned documents. Businesses are thus motivated to support trusted digital IDs if it means more reliable customer identification. Insurers or lenders may offer better terms if identity assurance is higher (some fintech in EU use the national digital ID to expedite loans).
- **New Business Opportunities:** Digital identity frameworks can enable new services – e.g., age-verified delivery, digital signing of contracts, tailored

e-commerce where users can share relevant data instantly. Companies might build products around the availability of verifiable credentials (for example, offering “instant credit” if you share your government-verified income credential). This can spur adoption as the ecosystem sees value creation opportunities.

Industry Standards and Interoperability (The Role of OIDF and Others)

As mentioned, **standards organizations and industry alliances are critical to digital identity interoperability**. The **OpenID Foundation (OIDF)**, for instance, is behind the OAuth2/OIDC protocols that power billions of authentication transactions. OIDF’s work on profiles like **OIDC for Verifiable Credentials (OIDC4VC)** and OIDC for Identity Assurance provides a common language for exchanging trustable identity data. This effectively helps different trust frameworks talk to each other. For example, OIDC4VC allows a verifiable credential to be issued or verified using the well-understood OAuth/OIDC flows, bridging SSI technology with web standards . The OIDF’s Identity Assurance spec maps to government-defined assurance levels (including eIDAS levels of assurance) , so a private company could request an “OIDC Identity Assurance Level 2” assertion and accept it whether it came from a government eID or a bank, because they follow the same spec. By providing these standards, OIDF effectively **lowers technical barriers and fosters an interoperable trust ecosystem**. It does not choose who to trust (that’s a governance question), but it ensures that if two parties decide to trust each other’s identities, they can do so with minimal integration work.

Other industry groups include the **Kantara Initiative** (with its Identity Assurance Framework), the **FIDO Alliance** (focused on authentication, providing standards like WebAuthn which are used for passwordless login and could be part of trust frameworks for high security), and the **Trust Over IP Foundation** (which is developing a multi-layer architecture for SSI including governance frameworks). The presence of these organizations indicates the recognition that **no single entity can solve digital identity alone** – it requires broad agreement on how to implement trust.

For businesses, aligning with industry standards means **future-proofing** their identity solutions. It avoids vendor lock-in and eases compliance if regulations adopt those standards. For policymakers, endorsing or referencing industry standards (like eIDAS referencing ETSI standards for signatures, or US NIST referencing OIDC/OAuth for federation) can accelerate ecosystem maturity.

European Blockchain Services Infrastructure (EBSI) – A Governance Pilot

The **European Blockchain Services Infrastructure (EBSI)** is a project by the EU (under the European Commission and EU member states) to leverage blockchain technology for cross-border public services, including digital identity and credentials. EBSI can be viewed as a **pilot environment for a new trust model**. It provides a **distributed ledger network operated by European governments**, on which certain data or registries can be stored in a tamper-evident way . One of the use cases EBSI has piloted is **verifiable diplomas**: universities issue diploma credentials to students, and an EBSI blockchain registry is used to record the **trusted issuers (universities) list** and perhaps the hash of issued diplomas for verification .

From a business/governance perspective, EBSI is interesting because it introduces a **pan-European trust layer not controlled by any single actor**. Instead, multiple accredited participants (universities, in the diploma case, or public authorities in others) write to the blockchain, and verifiers consult it to verify authenticity. The trust model here is decentralized but permissioned: only trusted organizations can write credentials or accreditations to the ledger . EBSI thus is experimenting with **trust lists in blockchain form** (Trusted Issuer Registry on EBSI) and with **verifiable credentials issuance**. It's essentially a **governance sandbox**: figuring out how to **onboard issuers** (there's a process to authorize an organization as a Trusted Issuer – they get a DID on the blockchain and an accreditation from a “Trusted Accreditation Organization” or TAO) . This governance model, defined in EBSI’s “Trust Framework”, creates a **hierarchy of trust** on the blockchain: a **Root Trust Anchor** (Root TAO) can accredit sectoral TAOs, which then accredit issuers in their domain . All these relations (accreditations) are themselves verifiable credentials recorded on the ledger . The result is that a verifier can query the ledger to see if a given credential’s issuer is accredited under an EBSI trust chain for that credential type, and thus decide to trust it.

For EU policymakers and industry, EBSI serves as a proof-of-concept that **decentralized technology can be governed in a multi-lateral way**. It informs the eIDAS 2.0 implementation (for example, the concept of **Trusted Accreditation Organizations** in EBSI pilots is very relevant to how to govern private issuers of attributes under the future EU wallet system). EBSI also provides a template for **cross-border governance**: since multiple countries partake, it shows that no single country needs to host the “one database”; instead, each can run a node, share responsibility, and rely on a common set of rules. This might become a blueprint for other data spaces.

In terms of business adoption, EBSI is still in pilot phase, but companies are watching it. If the EU eventually uses EBSI (or similar networks) in production for verifying, say, business licenses or educational credentials, then companies will interact with it when hiring or onboarding customers. The fact that it’s built on open standards (W3C, etc.) means that businesses could integrate it without proprietary software.

EBSI demonstrates a **governance innovation**: it tries to achieve decentralization *without losing accountability*. All issuers are known legal entities (no anonymous issuers), all accredited by governmental bodies, but the verification can be done automatically and peer-to-peer. It’s an attempt to combine the assurance of a hierarchical trust model with the resilience and scalability of a decentralized network.

Hierarchical vs. Decentralized Trust Structures

Throughout this report, we’ve touched on hierarchical (centralized) trust vs. decentralized trust. From a governance view, this isn’t an all-or-nothing choice; often a **hybrid** is used. For example, in EBSI as we saw, there is a **hierarchical accreditation** structure, but implemented on a decentralized infrastructure. In a traditional PKI, we have a strict hierarchy (root CA > intermediate CA > end-entity certificate). Hierarchies are straightforward to govern (there’s a clear chain of authority) but as some experts note, they have weaknesses: **single points of failure or control** at the top . If a root is compromised or influenced, the whole trust collapses . This was highlighted in the context of web PKI and even politically.

Decentralized or **“web of trust”** models (like PGP’s model, or SSI with multiple roots) avoid single points of failure but introduce complexity: each verifier must decide which issuers to trust, or rely on trust registries. Without a hierarchy, governance shifts to **network consensus or reputation**. That can be chaotic without some framework – imagine every verifier having to manually approve hundreds of issuer DID identities; not feasible. So in practice, even decentralized systems introduce *some* structure (trust registries, governance authorities, etc.).

The **business perspective** on this is pragmatic: companies will adopt whichever gives them enough assurance with minimal fuss. Many companies are comfortable with hierarchical models (they trust a CA for SSL, they trust a gov ID). But we see growing interest in more decentralized approaches when hierarchy becomes a bottleneck. For instance, if integrating 28 EU national eID systems separately is too cumbersome, a decentralized approach with one interface (like the EU wallet with common standards) is preferable, even if behind the scenes a federation is needed.

Some identity networks use **“mesh” trust** – e.g., the Global LEI (Legal Entity Identifier) system has multiple issuers of identifiers for companies, accredited by a central body (GLEIF), so it’s a hybrid mesh/hierarchy. Financial industry trust frameworks, like SAFE-BioPharma, had cross-certification (hierarchies that cross-trust each other). This shows governance can be arranged in various topologies.

Ultimately, the decision often comes to **control vs. flexibility**. A hierarchical trust structure gives a central authority (or a few authorities) significant control – which can ensure consistency and rapid policy enforcement (e.g., revoke a compromised issuer quickly via the root). A decentralized structure gives participants more autonomy and potentially more resilience (no single kill switch). Many countries opt for hierarchical for their national ID (control is important for sovereignty), but when building cross-border or cross-sector, hierarchical can get complicated (whose root is above whose?). That’s why cross-domain frameworks often become federated networks of roots – in effect, a *federation of hierarchies*.

Governance bodies need to clarify roles: who approves issuers, how trust lists are managed, how audits are done. For example, **eIDAS 2.0 will likely require audit and certification of wallet providers and perhaps credential issuers** (for qualified attestations). That is a hierarchical element (certification by an accredited lab or authority). Yet the usage is decentralized at runtime. So hybrid is the norm.

From an industry standpoint, it’s important that hierarchical elements in governance do not stifle innovation or competition. If only one or two bodies can become identity providers, you get less innovation than if a hundred can (assuming they meet requirements). The EU’s approach to allow private issuers of attributes, but under supervision, tries to balance this.

In summary, **hierarchical and decentralized trust models each have pros and cons, and real-world systems often blend them**. Effective governance might mean establishing a **root of trust for policy** (to set rules and ensure compliance) while allowing **technical decentralization for implementation** (to avoid chokepoints and enable scalability). Businesses will align with the model that regulators favor, and regulators are increasingly favoring models that enhance privacy and user control – which pushes the pendulum somewhat away from pure central hierarchy towards distributed trust, but always with some governance guardrails.

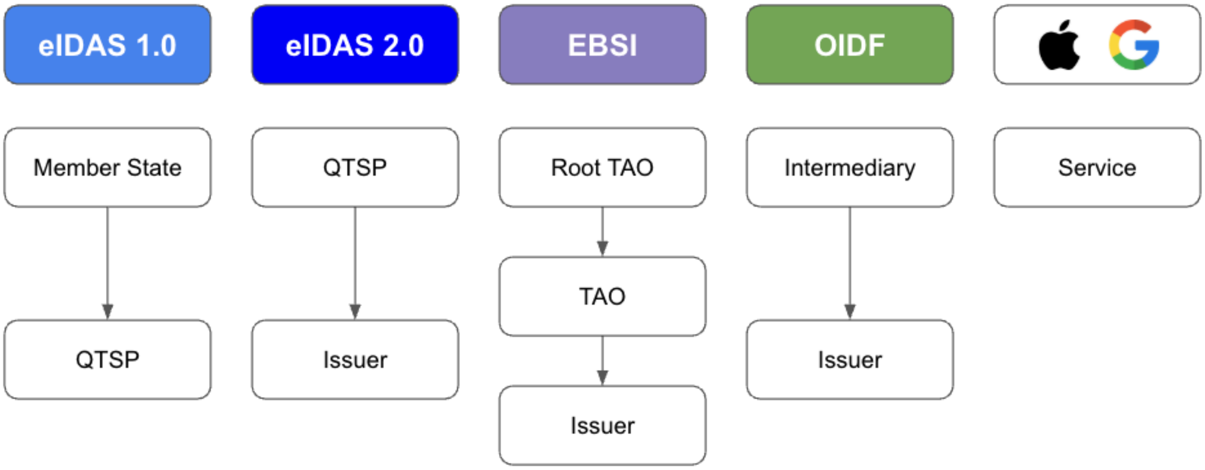


Figure 2

Challenges and Future Directions

As digital identity trust ecosystems continue to evolve, several challenges remain to be addressed, and various initiatives and standards are actively working to shape the future of trust models. In this final section, we outline key challenges – such as interoperability gaps, governance and liability questions, privacy and user adoption issues – and then explore how evolving standards and emerging technologies are likely to influence trust models in the coming years. We will touch on relevant standards efforts like **ISO's work on decentralized identity (ISO/TC 307 JWG4 and ISO 23042)** and trends like **verifiable credentials, blockchain-based identity, and self-sovereign**

identity (SSI) that are steering the direction of digital identity trust frameworks worldwide.

Interoperability Challenges

Interoperability – the ability of systems in different domains or countries to work together – remains a foremost challenge. Even within a single region, different sectors might use different identity standards (for example, healthcare vs. banking). Globally, the situation is even more fragmented. A user with a European Digital Identity Wallet credential, an Indian Aadhaar, and an American state-issued digital driver's license has three very different systems. How can a verifier trust all of these without integrating three or more verification processes? Lack of interoperability can lead to **"digital identity silos,"** where trust doesn't extend beyond a narrow domain.

Efforts to bridge these silos include developing **common data models and protocols**. The W3C's **Verifiable Credentials Data Model** is one attempt at a universal data format for credentials, which could wrap many kinds of claims. If widely adopted, any verifier could use a common library to verify credentials issued by anyone (given the issuer's public key and trust status). But beyond format, there is the issue of **policy interoperability**: does the verifier trust the rules under which the credential was issued? For example, a verifiable COVID vaccination certificate from Country A might be in the same format as one from Country B, but Country B might have less strict vaccination criteria; a verifier in Country A might not accept Country B's credential despite technical interoperability. This shows **governance interoperability** is as important as technical. Initiatives like the **Good Health Pass Collaborative** tried to address this by defining common principles and trust criteria for health credentials across jurisdictions . Similarly, the **Trust Frameworks for Identity Systems** whitepaper by OIX pointed out that many trust frameworks exist and the need for them to either map to each other or consolidate.

Another challenge is with **credentials crossing sectors**: An academic credential might be trusted by an employer but what about by an immigration officer? That might require linking an education trust framework with a government one. Projects like the **GAIN (Global Assured Identity Network)** proposed by some industry leaders envision a network where financial-grade identities (from banks) could be used in other contexts with mutual recognition. This is at concept stage but highlights the perceived need.

The future likely holds the creation of **meta-frameworks or interoperability agreements** – treaties or multi-lateral arrangements – so that a credential from one trust ecosystem can be *translated* or *gatewayed* into another. For instance, if the US and EU agree on recognizing each other's high-assurance credentials for travel or business, they might establish a liaison where a US credential can be issued also as an EU verifiable attestation or vice versa.

Technology can help by enabling **multiple trust roots**: for example, a digital wallet could carry a list of trust frameworks it complies with, or could hold multiple signatures on a credential (one from the issuer, one from a local authority bridging it to another framework).

Governance, Liability, and Trust Ecosystem Management

As trust models involve more players (especially in decentralized models), **governance structures** become more complex. Key questions arise: **Who is liable if something goes wrong?** If a verifier accepts a credential that turns out fraudulent, can they hold the issuer responsible? Under eIDAS, for example, qualified trust service providers have a legal liability (with reversed burden of proof) if their services fail . In decentralized models, such lines blur – if there is no central authority, every issuer might need insurance or users accept more personal risk. To address this, trust frameworks often include legal agreements or require participants to carry certain warranties.

Another governance challenge is **onboarding and maintaining participants**: who decides which issuers are trusted (and can be added to a trust registry)? This might be done by a governance authority or a collective (as in EBSI's case, a group of government bodies). Ongoing compliance needs to be monitored – e.g., ensuring issuers still meet security requirements, or revoking those that misbehave. This administrative overhead can be significant. Thus, establishing a **sustainable governance organization** – perhaps a non-profit consortium or a government agency – is crucial. The Pan-Canadian Trust Framework, for instance, is governed by the **Digital ID & Authentication Council of Canada (DIACC)**, a public-private body that sets criteria and approves components. Europe may set up a governance board for the EUDI Wallet ecosystem to coordinate Member States. These bodies will need to address disputes, evolve standards, and keep up trust lists.

User trust is also a governance aspect: if users don't trust how the system uses their data, they may opt out. Ensuring transparency (machine-readable policies, audit logs individuals can see) can help. Also providing recourse – e.g., if a credential is wrongly not recognized or revoked, how can a user or issuer appeal? Such processes need to be built in to maintain overall trust in the ecosystem.

Privacy and User Adoption Challenges

While improved privacy is a goal of newer trust models (through selective disclosure, etc.), there are still challenges to overcome. **Correlation** is a big privacy risk: if the same identifier is used everywhere, different verifiers could collude or correlate activity (a classic problem with any national ID number). Solutions include pairwise pseudonymous identifiers (as in some federation systems) or using **DIDs** which can be different per relationship. But implementing these in a way that regulators approve and that doesn't confuse users is a task. For instance, the EU Wallet may generate unique internal IDs per verifier to avoid tracking – that needs to be standardized so that verifiers handle it correctly.

Another privacy challenge is how to allow **account recovery or identity proofing without invading privacy**. For example, if someone loses their wallet, what's the recovery process that doesn't involve a central authority storing a backup of all credentials (which would reintroduce centralization)? This is partly technical (key recovery methods) and partly policy (maybe requiring multiple trusted parties to attest to your identity to recover).

User adoption was discussed earlier but to emphasize: trust models will fail if users find them too complex or not beneficial. The **value proposition** to the user must be clear ("Use this wallet, and you no longer need to upload documents or remember dozens of passwords, and your data stays in your control"). Education is needed, as many people are not familiar with concepts like digital certificates or self-sovereign identity. The terminology and UX need to be simplified – users shouldn't have to understand the cryptography under the hood. Initiatives in UX standards for wallets (like the Linux Foundation's ToIP UX guidelines) are working on consistent metaphors (e.g., the "wallet" and "credentials" metaphor itself).

Additionally, vulnerable populations or those without smartphones must be considered, otherwise digital identity can worsen digital divide. Policymakers often plan for alternate methods (like a printable QR code or an assisted service via post offices, etc., to onboard and support those users).

Evolving Standards

Standards development is a key part of future-proofing trust models. Two specific references are **ISO 23042** and **ISO/TC 307 JWG4**. ISO/IEC 23042 appears to be an emerging standard related to decentralized identity – according to Afnor, it's an

“Overview of existing DLT systems for identity management” . This suggests ISO 23042 might be a technical report surveying how blockchain and DLT are used for identity (perhaps similar in scope to the W3C DID spec, but from ISO perspective). By documenting existing systems, ISO can then identify areas to standardize. For example, ISO might set standards for **DID methods resolution** or **blockchain-based credential registries** to ensure different DLT identity systems can interoperate or at least be understood in common terms.

ISO/TC 307 is the technical committee on blockchain and DLT, and JWG4 is a Joint Working Group likely with ISO/IEC JTC 1/SC 27 (Security) or SC 17 (Cards and personal identification) focusing on identity. JWG4 is reported to be dealing with “Identity management and blockchain” which includes trust aspects. They are possibly standardizing things like **decentralized identity governance** or **quality criteria for DLT-based identity**.

Meanwhile, **ISO/IEC JTC1 SC 27** (which handles information security) has also been working on identity standards – e.g., ISO/IEC 24760 (A framework for identity management) and others, though those predate SSI. A new ISO standard **(ISO/IEC 18013-5)** covers mobile driver’s licenses – showing ISO’s involvement in mainstream credentialing.

The existence of these efforts implies that by aligning national systems to international standards, trust can be established more easily between them. For instance, if a country’s blockchain-based academic credential system conforms to ISO 23042 guidelines, another country’s verifier might be more willing to accept those credentials as they know it meets an international baseline.

Finally, the **W3C Verifiable Credentials 2.0** and **Decentralized Identifiers 1.0** standards provide the technical substrate for many new systems. As those stabilize and get adopted (perhaps even by ISO if they become ISO/IEC standards via JTC1 passthrough), they will likely serve as the “HTML of digital identity” – common data and method standards that everyone uses.

Trends

Looking ahead, several trends in trust establishment are likely to shape digital identity:

- **Verifiable Credentials (VCs) Everywhere:** The concept of VCs – tamper-evident, digitally signed credentials under the holder’s control – is being adopted not only in cutting-edge SSI projects but also by governments and enterprises. As we discussed, eIDAS 2.0 essentially mandates a VC approach. The U.S. DHS pilots use VCs. Banks are looking at VCs for sharing KYC between institutions. This trend means that the **triangle-of-trust model with issuer signatures** will become a standard mental model. Verifiers will increasingly expect a portable credential (as opposed to contacting an API every time) . We might see the decline of federated SSO in some areas in favor of direct credential presentation (already, technologies like **Microsoft Entra Verified ID** are offering VC-based identity for enterprise scenarios, complementing OIDC). Over time, a person’s digital wallet might hold dozens of VCs (ID, certificates, memberships, etc.), shifting how trust is managed – more at edges, less at central servers.
- **Blockchain and Distributed Ledgers:** Not all SSI systems use blockchain, but many do for certain functions like **decentralized PKI (DID registries)** or **credential status lists**. Blockchain’s role in trust models is to provide an immutable, decentralized way to store public information that multiple parties can rely on (like a list of trusted issuers, or a registry of revoked credentials). EBSI is an example, as is the Sovrin network historically. We can expect **more use of distributed ledgers as trust utilities** – e.g., national authorities might publish “issuer lists” on a public ledger rather than on a government website, for easier integration by verifiers globally. Blockchain can also automate aspects of governance via smart contracts (for instance, automatically expiring an accreditation at a certain date unless renewed, etc.). The flip side is performance

and scalability; blockchains need to handle potentially billions of transactions if used for widespread identity checks. There's ongoing work on scalable Layer-2 solutions and side-chains for identity. Another trend is use of **blockchain for user-controlled data consent** logs (some ID systems log each time data is shared, on a ledger, so the user and regulators have an audit trail).

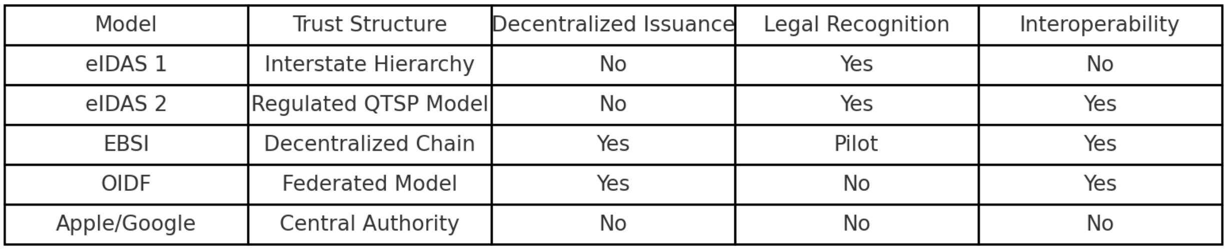
- **Self-Sovereign Identity (SSI):** SSI is as much a philosophy as a technology stack. The idea that individuals (and organizations) **should fully control their identity data** and decide who to trust, is influencing policy (e.g., EU's language about "giving control back to the user"). Over the next decade, we may see more convergence of government ID systems with SSI principles – as we already see in Europe. This could mean, for example, that even highly authoritative credentials like passports might become available as verifiable credentials that you hold and present without the issuing government tracking every usage. Technologically, this is feasible (a country's passport office could issue a VC of passport data into your wallet). Governance-wise, it requires acceptance by verifying authorities (like border control in another country – that's some way off, but pilots like Digital Travel Credentials by ICAO are already using a similar concept).

SSI also extends to **organizations controlling identity** (DIDs for companies, etc.), which could transform trust in supply chains or business credentials (a company could present a verifiable license or ISO certification to a client).

The concept of **"web of trust"** might regain popularity via SSI, where trust is more peer-to-peer or decentralized. Instead of one global root, you might have **trust communities** (Trust Hubs or Trust Registries). We see early versions with things like the **Trust Over IP Trust Registry Protocol** – which would allow querying if an issuer is trusted in a given context. That fosters a more dynamic trust model: you query different registries depending on context (one for healthcare, one for education, etc.). This specialization can increase trust within verticals, but it raises the question of bridging them (again, interoperability governance).

- **Artificial Intelligence and Identity Proofing:** Looking further ahead, technologies like AI might both help and challenge trust models. AI can assist in identity proofing (better facial recognition, fraud detection patterns) but also enable deepfakes that can fool systems. So trust frameworks will likely embed AI-driven verification (which then has to be trusted itself – requiring transparency of algorithms perhaps).
- **Post-Quantum Cryptography:** In terms of technical trust, there's a looming need to migrate identity systems to post-quantum crypto algorithms to remain secure in the future. Standards bodies (like NIST, ETSI, ISO) are working on new algorithms. Trust models might have to incorporate **algorithm agility** as a requirement (ensuring issuers use quantum-resistant signatures eventually, etc.).

In conclusion, the future of digital identity trust models is heading toward greater **user-centricity, interoperability, and security**, enabled by global standards and innovative technologies. We will likely see a world where an individual can seamlessly use digital credentials from one context in another (e.g., use a government-issued digital ID to prove age at a bar, or use a bank-issued ID to log into a government service), with the underlying trust being verified through common protocols and trust frameworks. Governance will play the pivotal role in tying these together – ensuring that different systems and models interoperate under agreed rules so that digital identity truly becomes a universal utility, much like the internet is for information.



Model	Trust Structure	Decentralized Issuance	Legal Recognition	Interoperability
eIDAS 1	Interstate Hierarchy	No	Yes	No
eIDAS 2	Regulated QTSP Model	No	Yes	Yes
EBSI	Decentralized Chain	Yes	Pilot	Yes
OIDF	Federated Model	Yes	No	Yes
Apple/Google	Central Authority	No	No	No

Figura 3

Conclusion

Digital identity trust models form the backbone of our digital interactions – from logging into websites, to accessing government services, to signing contracts electronically. In this report, we examined how these trust models are defined and implemented, focusing on Europe's journey from a centralized eIDAS 1.0 model to the decentralized, user-centric approach of eIDAS 2.0 and the European Digital Identity Wallet. We compared global approaches, noting that while Europe is pioneering a hybrid of government assurance and self-sovereign principles, the United States follows a market-led federated model, China enforces a centralized state-controlled model, and countries like Brazil and Mexico are developing federated frameworks to unify identity across sectors.

From a business perspective, we highlighted the importance of governance, interoperability standards, and clear value propositions to drive adoption. The involvement of industry groups like the OpenID Foundation and the piloting of new technologies through projects like EBSI demonstrate a collective effort to tackle the challenges of scaling trust across organizational and national boundaries.

Key challenges remain: aligning disparate systems, preserving privacy, clarifying liability, and achieving global interoperability without compromising local needs. Yet, ongoing work in international standards (such as those under ISO and W3C) and the rapid evolution of technologies like verifiable credentials and distributed ledgers are paving the way for more robust and flexible trust frameworks. The trends indicate a future where individuals and organizations can **seamlessly prove and trust digital identities across contexts**, with high security and minimal friction, all while maintaining control over personal data.

For policymakers and industry leaders, the imperative is to continue collaborating on open standards and reciprocal trust arrangements – much as eIDAS has done for

Europe – so that the patchwork of today's digital identity systems can be woven into an **interoperable fabric of trust**. The promise of digital identity is better security, efficiency, and inclusion; achieving it will require balancing the hierarchical structures that provide assurance with the decentralized innovations that provide agility and user empowerment. With thoughtful governance and broad stakeholder engagement, trust models for digital identity will undoubtedly mature, enabling a safer and more convenient digital economy for all.

Sources: The analysis in this document is supported by a range of sources, including official regulations, technical frameworks, and industry insights. Key references include the eIDAS Regulation and European Commission documents for the European perspective , NIST guidelines and U.S. government reports for the American context , legal analyses for China's system , and industry whitepapers and standards documentation that shed light on trust frameworks and emerging standards . These citations, indicated throughout the report, provide further detail and substantiate the points discussed, ensuring that our study is grounded in credible, up-to-date information.

References

1. **Trust Management Models for Digital Identities**

https://www.researchgate.net/publication/323251666_Trust_Management_Models_for_Digital_Identities

2. **Digital Identity: An Approach to Its Nature, Concept, and Functionalities**

https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaae019/7760180

3. **Assessing the Trustworthiness of Electronic Identity Management Systems**

https://arxiv.org/pdf/2502.10771

4. **SoK: Trusting Self-Sovereign Identity**

https://arxiv.org/pdf/2404.06729

5. **Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems**

https://arxiv.org/pdf/2105.15131

6. **Modeling an Identity Trust System (ISACA Journal)**

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/modeling-an-identity-trust-system

7. **World Bank Digital Identity Toolkit**

https://documents.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf

8. **World Bank: Digital ID Strategy in the Netherlands**

https://www.worldbank.org/content/dam/photos/1440x300/2022/feb/2021-05-13-Digital-ID-strategy-Netherlands---Worldbank-ID4D-Webinar.pdf

9. **Public Dialogue on Trust in Digital Identity Services (UK Government)**

https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report

10. **The Human Rights Implications of China’s Social Credit System**

https://ohrh.law.ox.ac.uk/the-human-rights-implications-of-chinas-social-credit-system/

11. **Trust Models Guidance – eDelivery (European Commission)**

https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Trust%2BModels%2BGuidance

12. **Q&A on Trust Services under eIDAS**

https://digital-strategy.ec.europa.eu/en/news/questions-answers-trust-services-under-eidas

13. **W3C Verifiable Credentials Data Model 2.0**

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

14. **The Three Models of Digital Identity Relationships (Evernym)**

https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

15. **Digital Identity and Trust (DHS Archive)**

https://www.dhs.gov/archive/science-and-technology/digital-identity-and-trust

16. **Digital Identity: The Current State of Affairs (BBVA Research)**

https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

17. **Digital Identity Trust (Equifax)**

https://www.equifax.com/business/product/digital-identity-trust/

18. **eIDAS 2.0: A Beginner’s Guide (Dock Labs)**

https://www.dock.io/post/eidas-2

19. **eIDAS 2.0: Everything You Need to Know (Ubiqu)**

https://ubiqu.com/eidas-2-0/

20. **Comparison Between Traditional and Decentralized Identity**

https://gataca.io/blog/comparison-traditional-decentralized-identity/

21. **eIDAS 2.0 Explained: Steps to Ensure Compliance**

https://gataca.io/blog/eidas2-explained/

22. **Everything You Need to Know About the EUDI Wallet**

https://gataca.io/blog/eudi-wallet/

23. **Guide to Verifiable Credentials and DIDs**

http://gataca.io/blog/self-sovereign-identity-ssi-101-decentralized-identifiers-dids-verifiable-credentials-vcs/

24. **Decentralized KYC in DeFi**

https://gataca.io/blog/decentralized-finance-self-sovereign-identity-a-tale-of-decentralization-a-new-paradigm-of-trust/