# uID: A Strongly-Secure Usable Identity Ecosystem

## 1. Executive Summary

This project will theoretically ground, build, and deploy key components of **uID**, a secure, usable, privacy-enabling digital identity ecosystem, able to integrate, and synergize with existing governmental, commercial and open-source identity and authentication solutions.

Designing tomorrow's digital identity solution is faced with unique challenges. Identity mechanisms overwhelmingly refer to and are used by people. They need to be *usable and affordable*, and address individual concerns of *privacy and confidentiality*. At the same time, to ensure trust they need to provide *accountability* and be strongly *secure*. Further, it is important to realize that no one platform can be a sole provider – a viable ecosystem will have standards with well specified APIs and conduits for interoperability that naturally foster a healthy market. Finally, it is essential that these mechanisms interoperate and are efficient so as to not constitute a bottleneck when deployed.

While addressing all of the above challenges, **uID** will focus on two *key* goals: privacy protection and transaction unlinkability. These properties are unfortunately conflicting and require a complex multi-layer research and development approach calling on multi-disciplinary expertise across all the layers of today's digital transactions. Simple "browser plugins" or "email-based" mechanisms alone are bound to fail by not considering the multiple cross-layer security challenges.

The **uID** prototype will be the result of a close collaboration between academic researchers, industry, and digital rights advocacy groups. This guarantees strong trust assurances, marketplace relevance and individuals' privacy protection. Further, **uID** will engage the open-source community early-on as a feedback and development base, to ensure wide community support and acceptance.

**uID** will demonstrate how to securely integrate existing identity providers, enforce individual privacy, and allow a wide range of users with different technological abilities to access and use their digital identity with ease. **uID** will result not only in practical usable software and hardware deliverables, but also in a research knowledgebase of reusable protocols, design recommendations, and proposals for standards which will be condensed as entries in a **Trusted Identity Charter**.

The ultimate goal of **uID** is to constitute not only a functional open-source preview of tomorrow's identity ecosystem but also a reference baseline for business and government-driven standards on interoperability, usability, privacy and security in the digital identity space in the years to come.

## 2. Project Approach

The main overarching goal of **uID** is to ensure accountable privacy and unlinkability. This is why it is important to first understand how identities are used in today's societies and what elements are essential in achieving these assurances.

Consider a typical transaction between an individual (or a software/hardware component with an identity) and a service provider (such as an online website). If the successful completion of the transaction *requires providing intrinsically identifying information* (e.g., IRS tax filing, online purchase of airline tickets etc) neither privacy/anonymity nor unlinkability can be achieved, notwithstanding any assurances of the deployed identity mechanisms. Naturally, the user may choose not

to participate in the transaction, but if she does, then the service provider will get access to the identifying information.

Further, if the transaction involves an individual, but no **Trusted Terminal** is available to allow the individual to interact as a client to the service provider, again, privacy and unlinkability cannot be achieved.

Even in the presence of a Trusted Terminal, since underlying network traffic reveals the location and IP address of the service client, **Anonymizers** such as Tor are required to preserve privacy and unlinkability. Yet, current anonymizers do not offer full unlinkability, especially when one considers the entire stack, including application-specific identifying information (e.g., browser or mail client version) that can propagate all the way to the service provider and can identify clients, often with very high accuracy. To mitigate this, **Anonymizers with strong unlinkability** assurances need to be devised, often having to include client-side plugins and logic eliminating or preventing applications' signatures from reaching service providers.

Once the terminals and communication conduits are shaped to allow for privacy/unlinkability assurances, **Anonymous Credential** mechanisms are needed to prevent service providers from identifying clients in the authentication and authorization phase, while still allowing them private access to services they are entitled to.

Yet, anonymity is not sufficient to guarantee unlinkability across multiple transactions. This is why it is important to design **Anonymous Credentials with unlinkability**.

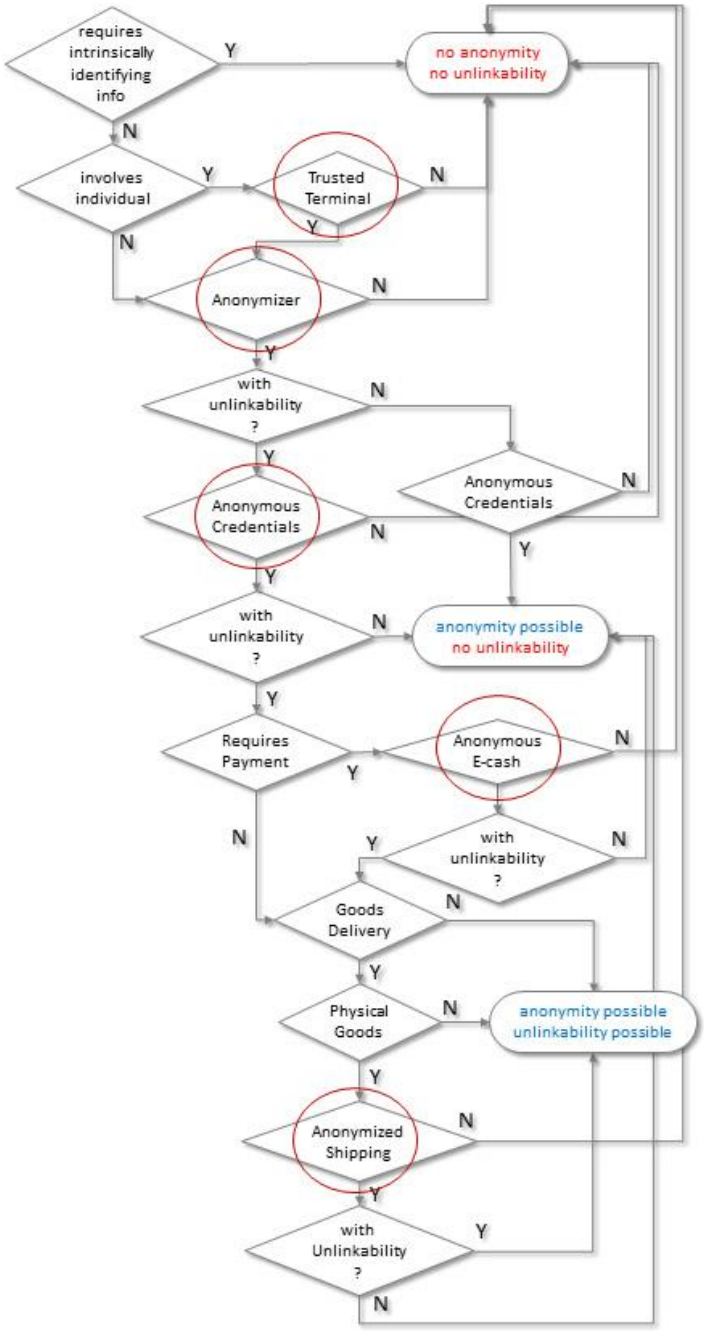


**Figure 1.** Identity Privacy and Unlinkability can only be achieved through a vertical approach integrating all transaction layers.

Further, full assurances are not guaranteed, especially if the transaction involves any form of payment, in which case **Anonymous Payment mechanisms with unlinkability** are also required.

Finally, if any goods are to be delivered to a physical address, **Anonymized Shipping** mechanisms will be required – to prevent service providers to directly infer client identities.

## 2.1. uID Philosophy: A unified cross-layer approach is essential

All of the above components – Trusted Terminal, Anonymizers, Anonymous credentials, Anony-

mous Payments, Anonymized Shipping – are necessary building blocks in a trusted identity ecosystem with transaction privacy and unlinkability.

This is why overall **identity privacy and unlinkability are not end-to-end solvable**, e.g., by a custom protocol, a "better web browser", a "software plugin" or other user-level tools alone. Instead, they require **a unified vertical approach addressing all the cross-layer privacy and unlinkability aspects**.

Unfortunately, a large percentage of today's systems and associated transactions miss these elements, which are essential in achieving a meaningful secure identity ecosystem. **uID** bridges this gap by bringing together experts in privacy, electronic payments, and large-scale systems, in the academic, government, industry and digital rights advocacy communities.

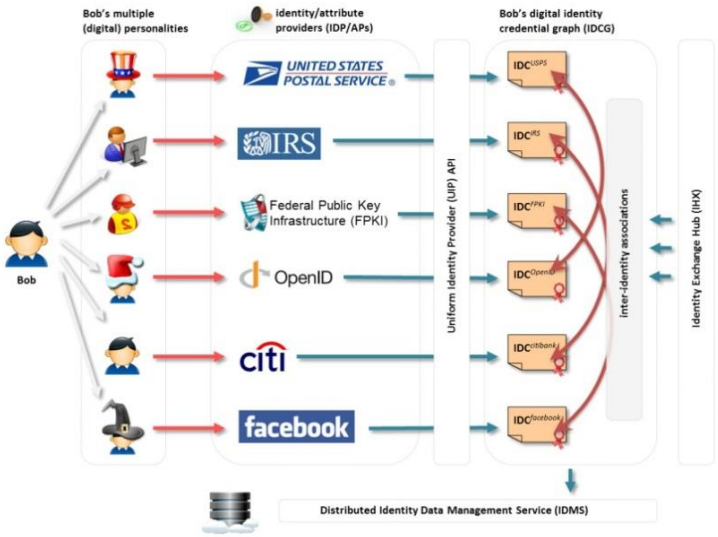


**Figure 2. uID** seamlessly integrates existing providers. Different identities are aggregated with privacy into an identity credential graph (IDCG) stored in-network by the Distributed Identity Management Service (IDMS).

## 2.2. Guiding Principles

### 2.2.1. Interoperability

The realization that no single identity solution can satisfy the technological and market needs of a viable identity ecosystem lies at the core of the **uID** vision. **uID** will be designed as an interoperability platform for any existing or future identity solutions. The pilot will demonstrate the integration of Google, OpenID, facebook, and Federal Public Key Infrastructure (FPKI) credentials among others. Further, integration of any new identity technology or platform will be achieved seamlessly by simply providing a short IDC XML meta-description of the platform's identity credentials. Interoperability and extensibility ensure not only wide adoption but also foster innovation and commercial opportunities, while providing structure and synergy in a currently fragmented landscape.

### 2.2.2. Strong Privacy

The IDC meta-identity will be designed from the ground up to not only integrate arbitrary existing credentials but also provide online pseudonymity as well as full anonymity when desired, on a voluntary, individual-choice basis. Further, the IDC "meta" encapsulator will have the capacity to provide anonymity and need-to-know disclosure (only minimum necessary information shared) *even for credentials stemming from legacy providers with no support for privacy*! As a result, end-to-end Fair Information Practice Principles (FIPPs) compliance, and strong privacy protection is ensured. The ultimate goal of the privacy controls will be to limit the collection and transmission of information to the minimum necessary to fulfill transactions and their related legal requirements; and to minimize data aggregation and linkages across multiple transactions.

### 2.2.3. Security and Resilience

**uID** will integrate with ongoing cyber security advances (several of which are driven by the team's member groups and institutions) and legacy mechanisms. Further, **uID** will also encompass a research and design thrust aimed at eliminating significant vulnerabilities that limit the resilience and security of today's server authentication mechanism. Specifically, in this thrust, novel highly scalable identity credential and authentication paradigms such as the Sovereign Keys concept will be

taken from the realm of research into a design and implementation phase. This will ensure not only high availability of authentication at scale but also eliminate the numerous vulnerabilities plaguing current PKI-based mechanisms such as SSL/HTTPS. Transactions will be more secure and accountable, identity mechanisms will be more available, and overall trust will increase.

### 2.2.4. Cost-Effectiveness and Ease of Use

It is virtually impossible to transact in today's highly digital societies without a meaningful minimal set of digital identities. This is why any feasible global-scale digital identity ecosystem will need to provide cheap (basically free in its most basic form), easy to get and easy to use identities. Further, the underlying core identity data management infrastructures are too important to the resilient operation of the identity ecosystem to be left in the care of any single commercial enterprise.

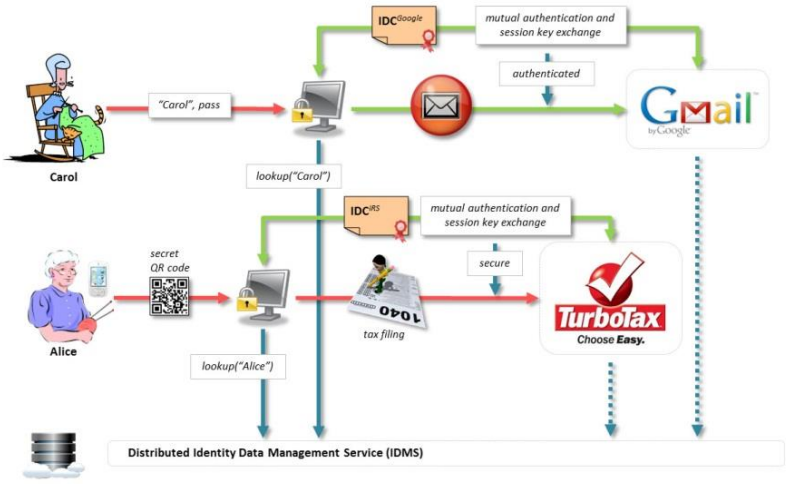


**Figure 3.** Individuals with different degrees of technological savviness will easily use their digital identity. Arbitrary authentication media and protocols will be supported, including smartphone near field communication, QR-codes, username/password, biometrics and smartcards.

This is why, in **uID**, while identity establishment and authentication will encompass an arbitrary number of providers and commercial/governmental services, the digital identity credential graph (IDCG) records (graph-structured identity and attribute data records of an individuals' multiple identities) will be managed *with privacy assurances* by a distributed identity data management service (IDMS), an in-network, *highly-resilient* service, similar to today's DNS domain name lookup service.

### 2.2.5. Adoptability

Most importantly, **uID** will **not require service providers to change their current authentication or authorization mechanisms**. We believe this is paramount for wide adoption. The Unified Usable Multi-Identity Manager coupled with the user's IDC encapsulator will deploy new techniques for **collaborative crowd-sourcing** to learn servers' authentication and authorization mechanisms automatically and allow the user to transact with a single click.

Further, **uID** will **operate across multiple platforms**, including different PC browsers and mobile devices. This is paramount to adoption in a high-tech society in which individuals are mobile, own multiple devices, and need to use different identities in different environments on a daily basis, e.g., at different work places, on the road, and at home.

Finally, **uID** will not lock customers into any single identity provider, but instead act effectively as a cross-provider integration platform.

**uID** will be not be solely a fundamental research effort but will focus on delivering multiple practical software deliverables that will seamlessly integrate in individuals' lives and run on today's web browsers and smartphones. Further, **uID** will put forward a **Trusted Identity Charter** – a set of concrete actionable proposals for universal identity ecosystem standards. **uID** will be open-source and will engage the community starting with the early design and development stages.