GAIN DIGITAL TRUST

How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Identity Network

With over 150 co-authors

The Contributors

Nacho Alamillo, Phil Allen, Peter Amrhyn, Martin Azcue Lopez, Daniel Babatola Awe, Simone Baldini, Fred Bär, Donna Beatty, Yoram Bechler, Waleed Beitar, Erik Belluci Tedeschi, Vittorio Bertocci, David Birch, Wayne Blacklock, Rod Boothby, Gijs Boudewijn, Matthias Bossardt, Andre Boysen, John Broxis, Katinka Jussie Lønning Bruberg, Nick Cabrera, Kim Cameron, Brad Carr, Peter Carroll, Anik Chawla, Daniele Citterio, Malcolm Clarke, Uli Coenen, Adam Cooper, Arthur Cousins, Cameron D'Ambrosi, Arthur Dallau, Scott David, Thibault de Valroger, Thomas Dübendorfer, Christian Duda, Andrei Dumitru, Vladimir Dzhuvinov, Thomas Egner, David Fennell, Daniel Fett, Conan French, Alexis Fruchaud, Justin Gage, Elizabeth Garber, Dominik Goergen, Daniel Goldscheider, Will Graylin, James Greaves, Odd Erling Håberget, Mark Haine, Patrick Harding, Gerard Hartsink, Mehraj Hassan, Joseph Heenan, Ben Helps, Bjorn Hjelm, Gail Hodges, Johs. Hoehener, Jens Holeczek, Carl Hössner, Stefan Imme, Martin Ingram, Brenan Isabelle, Ashish Jain, Vincent Jansen, Travis Jarae, Michael Jünemann, Marco Kaiser, Hitesh Kalra, Peter Kirkwood, Remy Knecht, Valentin Knobloch, Delia König, Adriaan Kruger, Martin Kuppinger, Julianna Lamb, Oliver Lauer, Rob Laurence, Row Lawrence, Gottfried Leibbrandt, Jörg Lenz, Johannes Leser, Emma Lindley, Gavin Littlejohn, Torsten Lodderstedt, Tobias Looker, Bianca Lopes, Douwe Lycklama, Maciej Machulak, Anil Mahalaha, Eve Maler, Piet Mallekoote, Viky Manaila, Jatin Maniar, Masa Mashita, Reed McGinley-Stempel, Karla McKenna, Tony McLaughlin, Simon Moffatt, Susan Morrow, Marcus Mosen, Nick Mothershaw, Hiroshi Nakatake, Axel Nennker, Michael Palage, Steve Pannifer, Radu Popa, Dima Postnikov, Dan Puterbaugh, David Rennie, Victoria Richardson, Robert Robbins, Andrea Röck, Timothy Ruff, Nat Sakimura, Michael Salmony, Samuel Scheidegger, Christoph Schneider, Schlager Ales, Frank Schlein, Rachelle Sellung, Sahil Shah, Somnath Shukla, Jesper Skagerberg, Tom Smedinghoff, Joerg Staff, Gabriel Steele, Frank R. Svendsen, Franco Tafini, Taavi Tamkivi, Antonio Taurisano, Oliver Terbu, Don Thibeau, Lars Gunnar Tiben, Andreas Toelke, Bob Trojan, Paiak Vaid, Andrea Valle, Francesco Vetrano, Jürgen von der Lehr, Liz Votaw, Marie Walker, Charles Walton, Laurence White, Edgar Whitley, Johannes Wirtz, Stephan Wolf, Dirk Woywod, Sudhindra Yapalparvi, Stuart Young

To cite this paper:

E. Garber, M. Haine, V. Knobloch, G. Liebbrandt, T. Lodderstedt, D. Lycklama, N. Sakimura et al., *GAIN DIGITAL TRUST, How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Identity Network*, European Identity and Cloud Conference, Munich Germany, September 13, 2021.

Executive Summary

The lack of verified Digital Identity presents an urgent problem and a meaningful opportunity for society. There are substantive risks to unfettered anonymity, ranging from the spread of misinformation to the enablement of criminal markets.[1] Meanwhile, to engage in the digital economy, individuals disclose myriad private data, including biometrics, with organizations that may sell, misuse, or lose it.[2] Yet, digital engagement is a key driver of economic growth - and inclusive participation requires access to high-trust identity verification services.[3]

The 150+ authors of this paper propose a shift towards a user-centric and high-trust identity paradigm: the Global Assured Identity Network (GAIN). Instead of logging in directly, an End-User asks a trusted and regulated provider (e.g., their bank, telecommunications provider, or another regulated entity) to verify that they are the person and/or have the credentials that they claim. Rather than managing over 100 passwords,[4] people will bring their identities with them and exercise greater control over data about them. This high-trust identity assurance, therefore, introduces an accountability layer to the internet even as it increases privacy and security.

Financial Institutions taking a lead in Digital Identity

This paper is directed at the leaders of Financial Institutions and is intended to catalyse a collaborative effort to develop the GAIN. Taking such action plays into core strengths, puts capital-hungry assets to work, and staves off disintermediating threats. Financial Institutions have done this before: they built global rails for trade, cards, digital payments, and securities.

Similarly, institutions whose leaders recognise that Digital Identity is a critical frontier for the global economy will drive this transformation. Underpinned by broad collaboration and strong principles, such as those put forward by the World Economic Forum,[5] it paves the way for greater inclusivity and access - even for today's unbanked populations.

The knowledge, skills, and technology exist to deliver the GAIN: it is now a matter of those with high-trust identity data - starting with Financial Institutions - joining together to unite disparate schemes and achieve the global reach required to underpin a truly digital economy.

Join the GAIN Proof-of-Concept

which will be shared at the 2021 IIF Annual Membership Meeting on 14 October in Washington, DC

Under the auspices of:

Cloud Signature Consortium
Global Legal Entity Identifier Foundation
Institute of International Finance
Open Identity Exchange
OpenID Foundation

Please contact DigitalTrust@iif.com to register interest.

Understanding Key Terms

While the main body of this paper seeks to avoid jargon, there are many references to participants in the identity ecosystem. For the purposes of this paper, the following terms have been used based upon international standards (ISO/IEC 24760 1) wherever possible.[1]

Term	How the term is used in this paper
Identity Information Provider	An entity that makes identity information, i.e., a set of attributes, available to Relying Parties.[5] *For example:* a bank may act as an Identity Information Provider because it has verified its customers' identity information using government issued identity documents. It may pass that information, such as age, name, address, to other entities.
Relying Party	An organization that wishes to ensure that an End-User is the person they claim to be and is entitled to an activity, based on identity information. Thus, they consume information from Identity Information Providers for the purpose of providing services to their End-Users. *For example:* a liquor store needs to know that a customer is the true owner of an ID document, e.g. a driver's licence, that shows they are over a minimum age.
End-User	A natural person that wishes to have an Identity Information Provider share identity information with a Relying Party.

[1] Note that more precise terms are defined in Appendix C.

Chapter 1: The Value of a Global Assured Identity Network

Key Points from Chapter 1:

- Trust between parties is critical to our global economy, but - as evidenced by rising data breaches, privacy concerns, and financial crime - trust online is broken.
- Financial Institutions have historically built infrastructures that underpin trust: together and with partners, they can develop a solution that benefits a wide range of stakeholders.
- The Digital Identity landscape is fragmented and 2 important factors will determine success: trust and reach.
- To realise benefits and stave off disintermediation, Financial Institutions must collaborate quickly to deliver high trust with global reach.

The Digital Trust Challenge

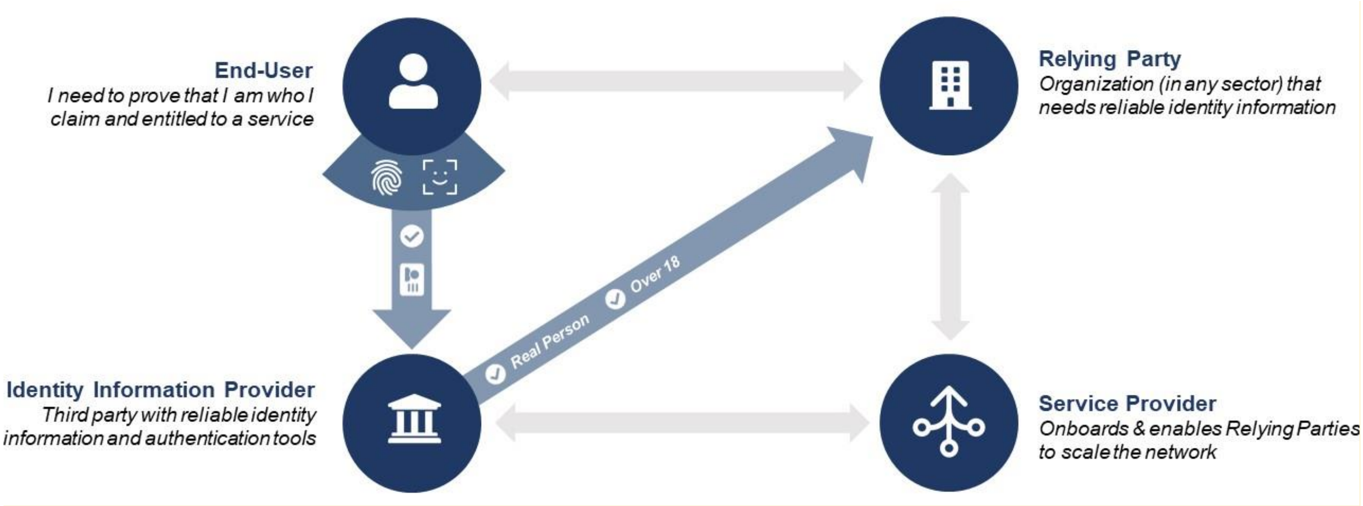
As transactions shift online, society faces a Digital Trust challenge: how to reliably and seamlessly identify one another while keeping private information safe. Financial crime, borne of illicit activities with untold human impact, amounts to an estimated 2-5% of global GDP per year[6] ($800 billion - $2 trillion USD[7]). These criminal markets often depend upon digital infrastructures that are anonymous by design or vulnerable to attack. It is in this context that Digital Identity is increasingly cited as a national security issue.[8] Meanwhile, it is also described as a pillar of growth[9] - one with the potential to expand access,[10] bolster human rights,[11] and grow the global economy.[12] In the absence of robust Digital Identity solutions, individuals and organizations (of any size) bear the cost: they carry the risk that someone is not who they claim to be, that their identities will be stolen,[13] or that private information about them will be used in unexpected - often perceived as unethical - ways.[14]

Establishing and maintaining Digital Trust infrastructure, therefore, is at a critical frontier of global economic innovation.[15] Chapter 1 of this paper shows that Financial Institutions have an opportunity to create and absorb significant value by offering high-trust identity services, and that doing so requires collaboration on a global scale. Chapter 2 lays out the critical next steps that will make it happen.

Benefits to Financial Institutions

Financial Institutions will reap many benefits from catalysing an interoperable global identity network: the first is strategic.[16] They face disintermediating threats on multiple fronts.[17] Large technology firms have global reach and are firmly entrenched in people's lives. Meanwhile, many more players compete for slices of an increasingly disaggregated value chain. Bank leaders argue that their competitors benefit from the uneven playing field that is created by a fragmented, entity-based approach to regulation and the one-way data flows mandated by regulators in some jurisdictions.[18] Yet Financial Institutions have the opportunity to offer Digital Identity solutions that address these concerns. Specifically, Figure 1 shows how Financial Institutions' investments in Know Your Customer (KYC) and digital authentication enable them to verify information on behalf of the organizations that need high-confidence data to offer services, referred to herein as 'Relying Parties.'

Figure 1: *Financial Institutions Answer Key Questions as Identity Information Providers*


End-User
I need to prove that I am who I claim and entitled to a service
Relying Party
Organization (in any sector) that needs reliable identity information
Real Person
Over 18
Identity Information Provider
Third party with reliable identity information and authentication tools
Service Provider
Onboards & enables Relying Parties to scale the network

Such networks show promising results in regions where they operate (see side panel). When they facilitate these transactions, Financial Institutions maintain their day-to-day relevance with consumer and business customers.

Benefits extend further - and many could be realised within two years. Digital Identity solutions create efficiencies for Financial Institutions: they turn a cost-centre into a profit-centre, simplify processes (login, password recovery, customer onboarding, signing), and enable cross-border platforms that facilitate scale. Ongoing efforts to remove barriers (e.g., data sharing within and between institutions) and to move towards comparative legal and regulatory structures will serve to expand the total opportunity.

As Chapter 2 will show, working groups and a proof-of-concept are mobilising now for a late 2022 launch. Institutions will begin realising benefits soon and, by building this ecosystem, may instigate the shift toward frameworks that maximise return and support globally-scaled platforms more broadly.

Results from Established Trust Networks

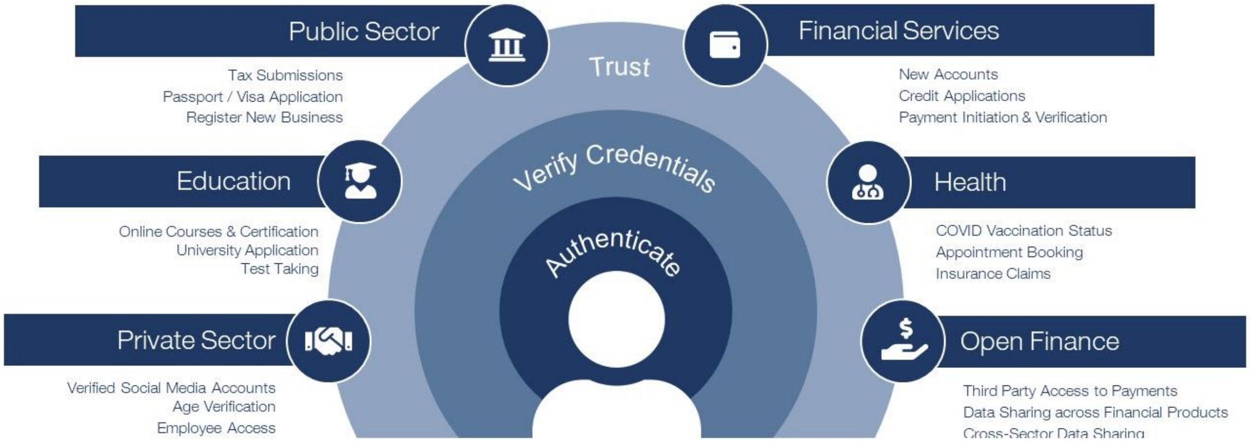
- BankID Sweden achieves 840 interactions per user per year - and is used by over 98% of those aged 21-67.
- BankID Norway has 99% market penetration within the adult population and 215 transactions per user per year.
- Over 1000 German banks form the yes® network.
- itsme® in Belgium has onboarded over 60% of the population: the Digital Identity app offers identification, authentication, confirmation, and digital signatures.
- Over 17m Canadians use Verified.Me (powered by the banks) at 85 federal government services; its use is expanding across the economy.

Financial Institutions within the Competitive Landscape

These advantages are fully realisable if Financial Institutions work together. The established networks (above) have shown that banks are able to create and absorb value in the identity ecosystem because of the unique strengths that build trust and underpin their core offer today. They are in the business of trust: since the founding of the Medici Bank in 1397, they have pioneered the development of trust infrastructures that enable trade between distant parties and across borders. As described above, they are bound by KYC regulations to invest in verifying the identities of their customers. They have a fiduciary responsibility to keep that data private and invest in security. This is why, although numbers vary by jurisdiction, Financial Institutions are some of the most trusted across the world on matters of data and security.[19]

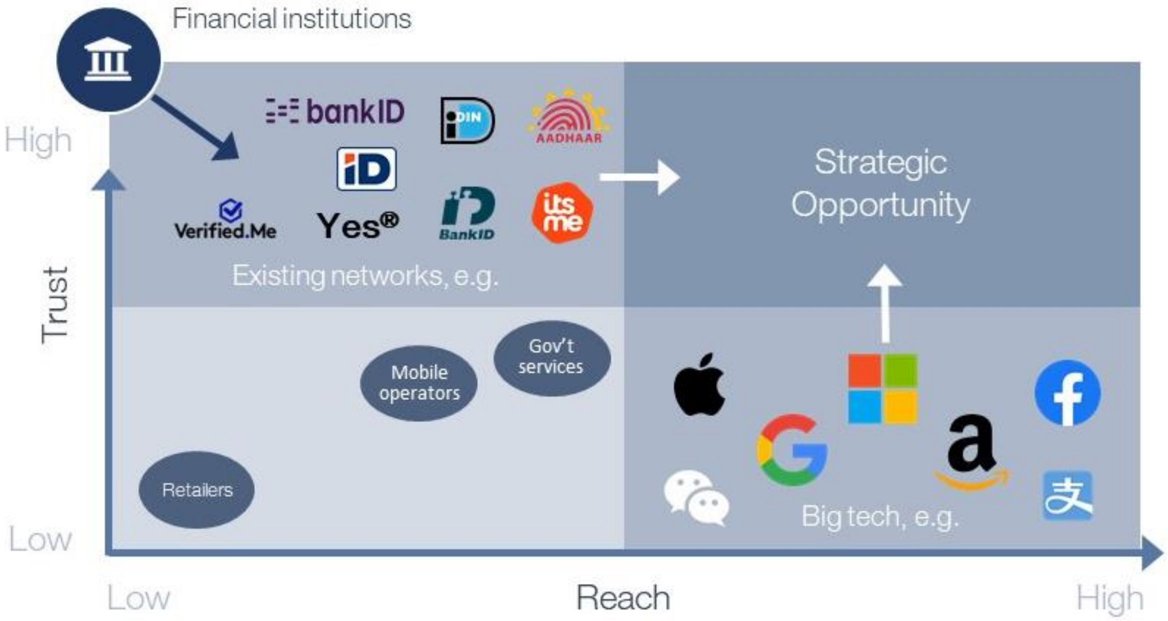
This high degree of trust establishes Financial Institutions' market opportunity. They offer End-Users security, control, and convenience. Meanwhile, Relying Parties benefit from, not only 'Financial-Grade' Identity Assurance, but also a dramatically simplified user experience. As End-Users enjoy an easier online life with far fewer passwords and forms, Relying Parties will improve their conversion rates and contain servicing interactions in digital channels.[20] As shown in Figure 2, such a network adds value for Relying Parties across the economy: energy, insurance, health, education, mobility, and beyond (Figure 2). More details about the Value Proposition to End-Users and Relying Parties can be found in Appendix A.

***Figure 2:** Use Cases in the Identity Ecosystem*



However, Relying Parties require cross-border collaboration between Financial Institutions – and other high-trust Identity Information Providers (e.g., public sector, energy, telecommunications) – to realise benefits. Since Relying Parties cannot contract and integrate with every Identity Information Provider, they need a network. Since they operate internationally, with customers and suppliers in many countries, that network must be globally interoperable. Global reach, therefore, is critical to success (Figure 3): without it, the benefits to Relying Parties and End-Users diminish.

Figure 3: *The Dynamic of Trust and Reach*



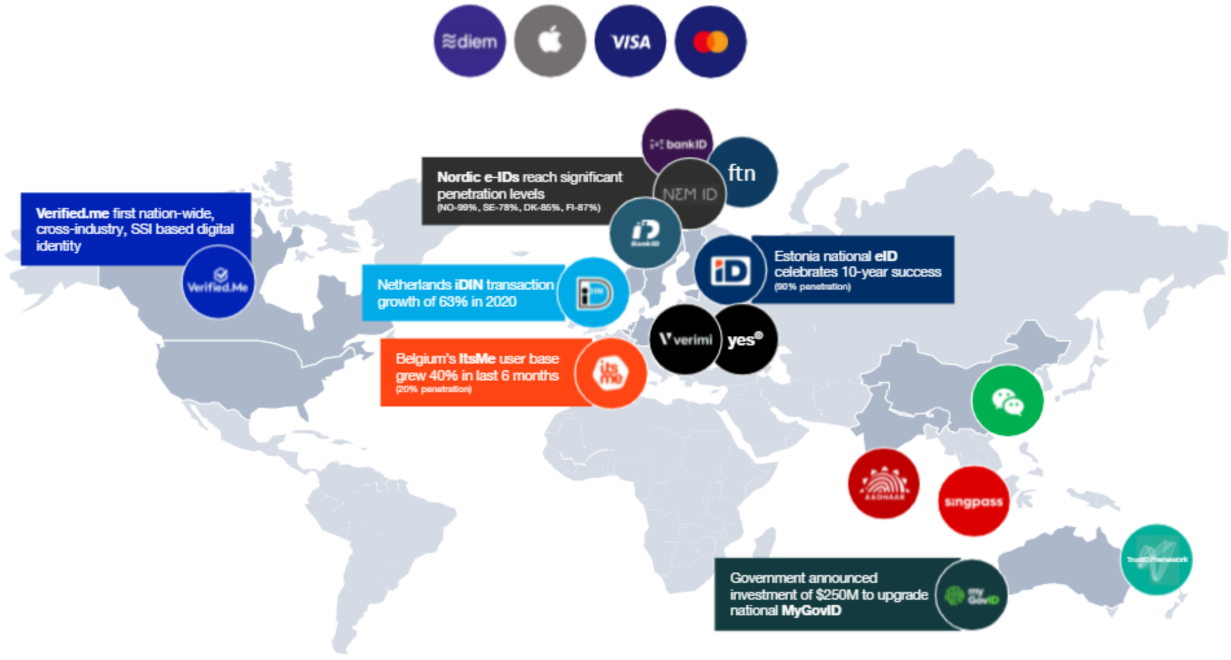
As shown in Figure 3, strategic relevance depends upon the dynamic between 2 factors: Trust and Reach. Large technology firms provide a simple experience that has led to broad adoption and global scale. Their current capabilities, however, do not extend to contexts requiring a high-degree of certainty about an individual's identity. Financial Institutions, by virtue of their investments in KYC and authentication, offer a high-degree of Trust. However, alone or as discrete in-country networks, they do not have the reach to provide Identity Information to Relying Parties that operate globally. To achieve that scale requires collaboration between those institutions with high-trust identity information: Financial Institutions and other regulated (or otherwise trusted) entities around the world.

By catalysing a decentralised and interoperable global network, as has been achieved for payments, Financial Institutions will offer high-trust identity assurance within a safe, sufficiently regulated environment: a major step toward Digital Trust.

Time is Running Out

Global reach requires interoperability akin to the global rails that connect localised payments, securities, and mobile communications solutions: this demands collaboration between institutions. A series of seminal publications have called on banks to collaborate on this type of high-trust identity solution - the World Economic Forum's *A Blueprint for Digital Identity*, [21] David Birch's *Identity is the New Money*, [22] Citi's *The Age of Consent*,[23] and McKinsey's *Digital Identification: A key to inclusive growth*.[24] Meanwhile, the solutions that have emerged (e.g., in Norway, Germany, Australia, Sweden, The Netherlands, Belgium, and Canada) prove that demand for financial-grade identity assurance exists.

***Figure 4:** The Fragmented Global Identity Market*



Verified.me first nation-wide, cross-industry, SSI based digital identity

Nordic e-IDs reach significant penetration levels (NO-99%, SE-78%, DK-85%, FI-87%)

Netherlands **iDIN** transaction growth of 63% in 2020

Belgium's **ItsMe** user base grew 40% in last 6 months (20% penetration)

Estonia national **eID** celebrates 10-year success (90% penetration)

Government announced investment of $250M to upgrade national **MyGovID**

The ecosystem in Figure 4 remains fragmented: a lack of interoperability constrains scale and adoption. In turn, the absence of scaled high-trust identity assurance constrains the benefits to all actors. Relying Parties must negotiate many contracts and integrate multiple systems to reach their customers. Each End-User experiences limited opportunity to verify credentials digitally.

Competitors recognise the gaps in this market and are mobilising: the time for Financial Institutions to act is now. Recent market movements reveal that key players are laying the groundwork to compete in a global high-trust identity market (see right) and major venture capital firms (e.g. Andreessen Horowitz, Accel, Felicis Ventures[25]) are expanding their investments in this space. At the same time, governments and regulators aim to roll out more digital services across society while users flock to the most convenient, readily-available experiences. In this context, non-financial actors will soon establish themselves in providing Digital Trust.

Market Movements

Recent movements in the identity market

$850M Mastercard acquired Ekata

$6.5Bn Okta acquired Auth0

$4.5Bn Clear Secure Inc IPO

$1.75Bn Trulioo valuation at Series D

The financial industry faces a choice: will customers ultimately login to their bank with a social media ID or will they use their bank to gain access across the internet? For Financial Institutions to address strategic challenges and create value for actors across the ecosystem, now is the time to expand the reach of their strongest asset: trust.

The time for cross-border, cross-sector collaboration is here.

Get Involved

We’re building a Global Assured Identity Network by the end of 2022.

Please contact **DigitalTrust@iif.com** to participate.

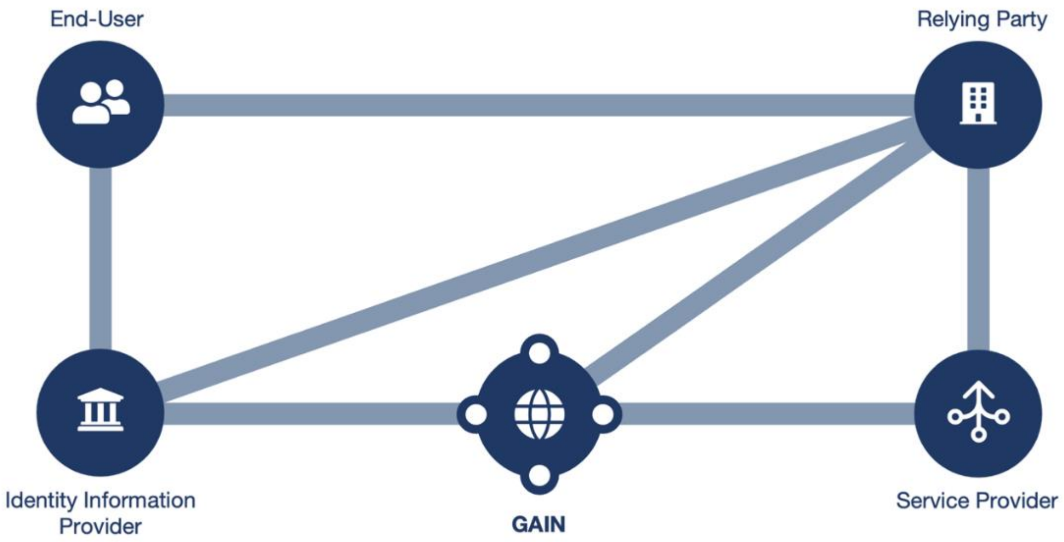
Chapter 2: Delivering the Network

Key Points from Chapter 2

- With a modest investment of time, money, and people, Financial Institutions can deliver a functioning Global Assured Identity Network (GAIN) that addresses key stakeholder needs by the end of 2022.
- This solution will be technically interoperable across borders and sectors of the economy.
- Please contact **DigitalTrust@iif.com** to register interest in participation.
- Appendices A-D propose value propositions, business models, details of the Trust Framework, and the technical architecture.

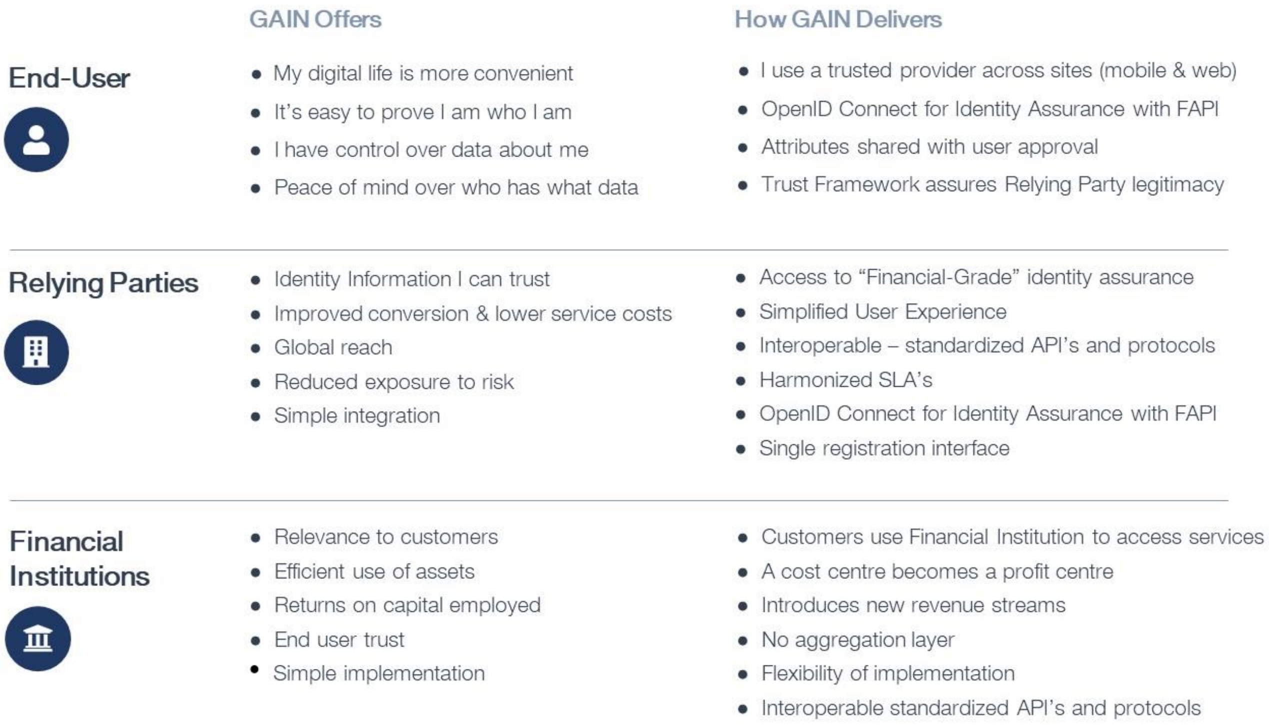
As established in Chapter 1, Financial Institutions have a window of opportunity to catalyse a decentralised, globally collaborative, and technically interoperable identity network that will benefit all parties and position them to compete. Chapter 2 provides a broad definition of the GAIN, with greater detail in Appendices A-D. Furthermore, it elucidates how Financial Institutions, Relying Parties, and key technology partners will come together to, with a modest investment of money, time, and human capital, launch the GAIN by the end of 2022.

Figure 5: *Relationships within the Global Assured Identity Network (GAIN)*



The GAIN delivers global reach to high-trust Identity Information Providers from any sector and enables them to act as one. It achieves this because it is flexible: it works with many architectures and is designed to complement the legacy infrastructures of its “Members.” Furthermore, it allows for different levels of assurance and enables compliance across a range of use-case and jurisdictional requirements.

Table 1: *How GAIN Delivers Value*



	GAIN Offers	How GAIN Delivers
End-User	• My digital life is more convenient • It’s easy to prove I am who I am • I have control over data about me • Peace of mind over who has what data	• I use a trusted provider across sites (mobile & web) • OpenID Connect for Identity Assurance with FAPI • Attributes shared with user approval • Trust Framework assures Relying Party legitimacy
Relying Parties	• Identity Information I can trust • Improved conversion & lower service costs • Global reach • Reduced exposure to risk • Simple integration	• Access to “Financial-Grade” identity assurance • Simplified User Experience • Interoperable – standardized API’s and protocols • Harmonized SLA’s • OpenID Connect for Identity Assurance with FAPI • Single registration interface
Financial Institutions	• Relevance to customers • Efficient use of assets • Returns on capital employed • End user trust • Simple implementation	• Customers use Financial Institution to access services • A cost centre becomes a profit centre • Introduces new revenue streams • No aggregation layer • Flexibility of implementation • Interoperable standardized API’s and protocols

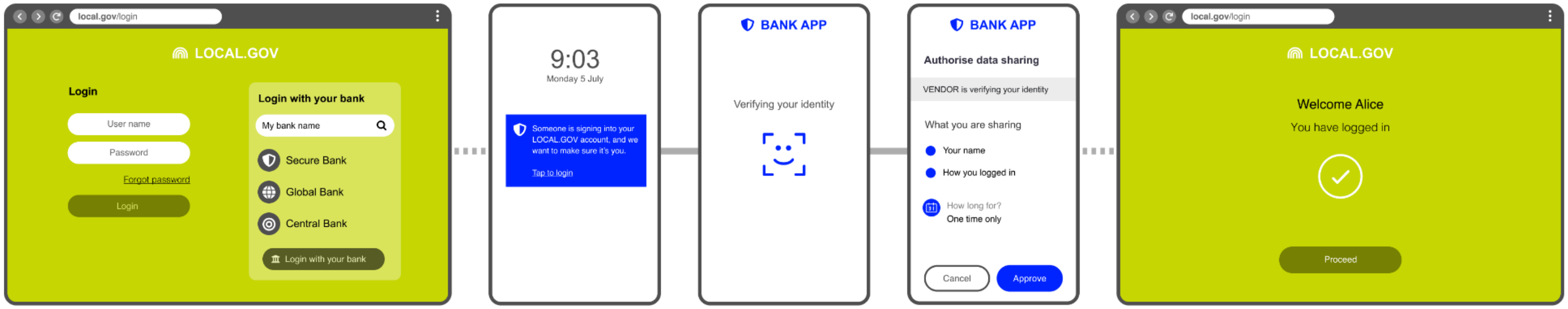
Note: For more information, Appendices A through D provide foundations for the GAIN proposition, multi-party business models, a Trust Framework, and technical architecture.

To ensure adoption, the GAIN user experience must be simple: designed to meet the fundamental needs of End-Users, Relying Parties, and Identity Information Providers. End-Users need only select their Financial Institution from the list of GAIN Members and may have an option to store a preference. What follows is an experience defined by the brand and the interface that they already use day-to-day - this may be their bank, another institution, or an existing assured identity scheme (e.g., itsme®, BankID, Verified.Me) and could be via web or mobile channels.

Illustrative GAIN User Experience

The GAIN does not have any direct interaction with an End-User: Relying Party and selected Identity Information Provider channels deliver the experience. The GAIN does, however, provide a mechanism for selecting the Identity Information Provider in the relevant Relying Party channel.

Figure 6a: *Alice is logging in to a local government service*

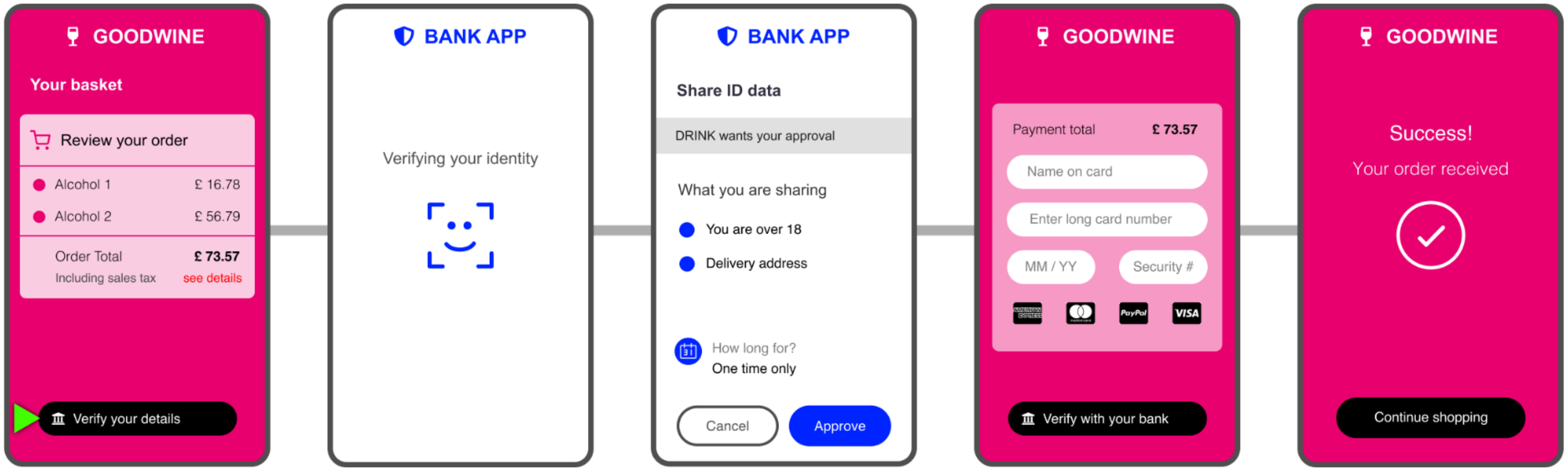


Someone is signing into your LOCAL.GOV account, and we want to make sure it's you.

Authentication	Authorisation	Attributes Shared
Alice receives notification to authenticate via her mobile app	Alice approves sharing of key attributes to the Relying Party (Local.gov)	*identifier,* *name,* *assurance level,* *authentication level*

Note: This is intended to show a government use case requiring a low Level-of-Assurance (LOA). The GAIN will support cases requiring a higher degree of identity assurance if the local jurisdiction allows.

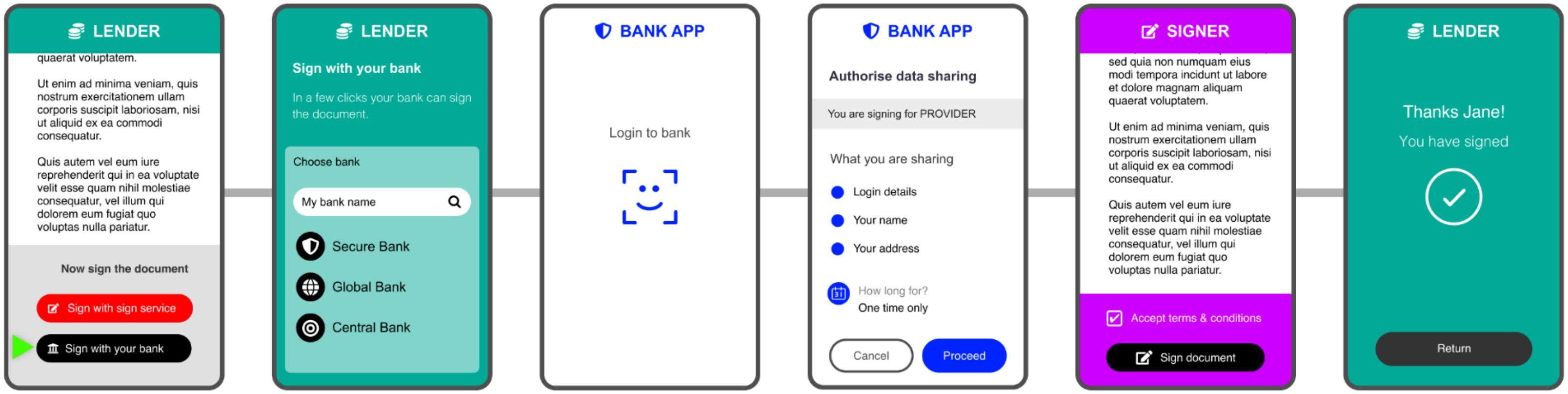
***Figure 6b:** Bob wants to buy alcohol and needs to login, prove his age, and confirm his delivery address*



Authentication	Authorization	Attributes communicated
Goodwine redirects Bob to his Bank’s mobile app based on cached preference	Bank app presents what data “Goodwine” is requesting Bob approves the sharing of requested attributes to “Goodwine”	*pseudo identifier,* *assurance level,* *authentication level,* *over-18-flag,* *address*

Note: the Identity Information Provider Chooser has been omitted from this journey on the basis that “Bob” has used this service and the Goodwine app has a locally cached preference for his preferred Identity Information Provider.

***Figure 6c:** Jane is setting up a new account and signing loan documents*



quaerat voluptatem.

Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur.

Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur.

sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem.

Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur.

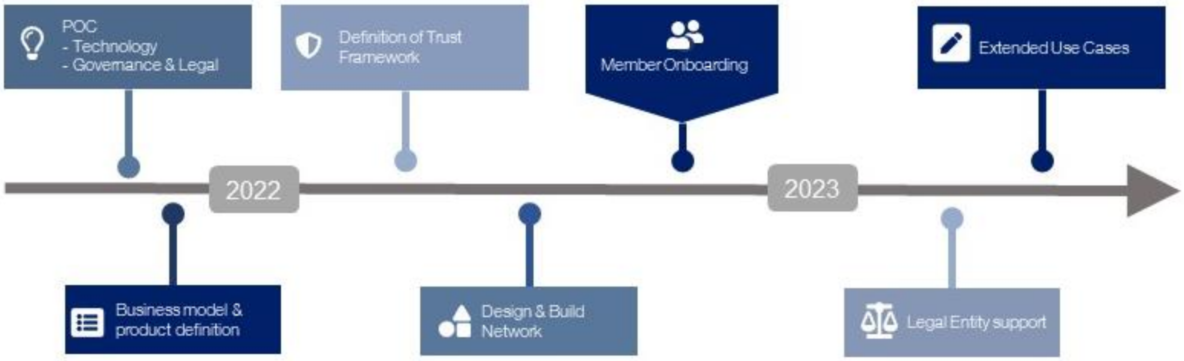
Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur.

Authentication	Authorization	Attributes communicated
The lender redirects Jane to her Bank’s mobile app	Bank app presents the data that “Lender” is requesting Bob approves the sharing of requested attributes to “Lender”	*identifier,* *name,* *assurance level,* *authentication level,* *address*

Once it launches in 2022, the experience of joining the GAIN will be similarly simple for Identity Information Providers and Relying Parties. They will require a single contract and integration: at that point, Identity Information Providers will begin serving the ecosystem. Relying Parties will be able to verify any customer's identity attributes (as long as they have a relationship with a Service Provider). All participants, including Financial Institutions acting as Identity Information Providers and/or Relying Parties, will begin realising the benefits of a globally interoperable network as early as next year.

To achieve this bold goal, however, requires a worldwide collaborative effort involving Financial Institutions, Identity Information Providers, Service Providers, and Relying Parties: **this has started already.**

Figure 7: *Milestone plan*



Conclusion

The GAIN creates new tools to verify people online: *are they human? Are they the person they claim to be? Are they entitled to this service? Are these payment details accurate?* These tools are available to individuals, industry, and further extend the options available to policy-makers.

Leaders who share this vision are invited to join the GAIN Proof-of-Concept, which brings together Financial Institutions, Identity Information Providers, Relying Parties, and key partners. They will co-create the GAIN product design, business models, technical architecture, and Trust Framework (building upon and adapting the proposals in Appendices A-D). This collaboration ensures that Identity Information Providers will secure sufficient reach to realise the benefits in Chapter 1.

This is only the beginning: by catalysing this movement, Financial Institutions will bring about a fundamental shift in the digital economy. As mentioned at the start of Chapter 1, Digital Identity is at a critical frontier. As the GAIN ecosystem expands, it will create new sources of value for all actors and for society at-large. In the medium-term, this may include value-added-services like insurance, signing, and the integration of Open Banking. Beyond this, the GAIN holds promise for society: not only does it address flaws in the online environment that lead to misinformation and crime, but it also expands access for millions around the globe. To deliver these gains, however, requires diverse working groups, broad participation, and a commitment to fundamentally inclusive outcomes.

Join the GAIN Proof-of-Concept

which will be shared at the 2021 IIF Annual Membership Meeting on 14 October in Washington, DC

Under the auspices of:

Cloud Signature Consortium
Global Legal Entity Identifier Foundation
Institute of International Finance
Open Identity Exchange
OpenID Foundation

Please contact DigitalTrust@iif.com to register interest.

Appendices

The 150+ authors have come together in broad agreement of the following proposals for how the GAIN ecosystem can become a reality. There will be important areas of disagreement, discussion, and further development: this is why you are invited to join the Proof of Concept.

Contents

Appendix A - Value Proposition Proposal[26]

The purpose of this section is to articulate, in greater detail, how GAIN can deliver value to End Users, Relying Parties, and Identity Information Providers. With Proofs-of-Concept, Working Groups, and inclusive collaboration, they will evolve.

A.1 End-User Value Proposition

Simplify your digital life: now you can use a trusted institution that safeguards your data to access almost anything.

Value for End-Users means…	How GAIN Delivers
Customer Jobs-to-be-Done	The Core Product & Services
• Prove that I am who I say I am • Access services that require information about me • Login to sites and apps across platforms • Access non-digital services requiring my information • Recover login details • Prove that I have credentials for an activity • Prove that I am entitled to a given activity • Sign - or formally agree to services* • Send and receive payments*	• Use Bank KYC data to provide evidence of identity • Share relevant data, easily, with my consent • Login to any service (feasibly) with my bank app • Use GAIN in offline venues too (i.e., QR codes) • I use my bank app to recover login details • Attributes may include certifications and entitlements • Information from the Identity Information Provider is used when signing* • Validate payment instructions & identities*
Customer Gains	Gain Creators
• Data sharing subject to consent & under my control • Reduce friction across experiences • Save me time • Confidence that data about me is secure • Enable me to maintain anonymity in certain spaces • I trust the people validating my identity/credentials	• I consent to each item shared • I can use my bank authentication almost anywhere • Fewer services require me to visit in-person • I trust my Financial Institution with my data • I need not consent to pass identifying information • Relying Parties adhere to GAIN's Trust Framework
Customer Pains	Pain Relievers
• Inconvenience • I have countless IDs/Passwords in my life • Things take too long / require too many documents • Service providers store too much personal info • Password recovery is hard • I must physically sign stuff • Are the payment details right? (sending & receiving) • Who is getting data about me, and can I trust them? • Fear of data breaches	• I can use my trusted Identity Information Provider to: ○ reduce the number of login credentials I need ○ sign up to new services online ○ consent to what data is shared ○ recover passwords ○ sign documents* ○ validate payment information* • Relying Parties adhere to GAIN's Trust Framework • I trust my Identity Information Provider

**These items are an extension of the initial GAIN launch: they are not planned for Day 1, and are not included in the forthcoming Blueprints.*

A.2 Relying Party Value Proposition

Identify and authenticate your customers - wherever they are in the world - with a simple, high-trust experience. Increase conversion; reduce the cost and complexity in your business.

Value for Relying Parties means…	How GAIN Delivers
Jobs-to-be-Done • Authenticate End User • Validate the identity, credentials, or entitlements of End-Users • Onboard and serve End-Users • Prove its authenticity and entitlements to its End-Users • Allow for levels of assurance to fit different use cases • Fulfil regulatory (e.g., data protection) requirements	The Core Product & Services • Identity Information Providers authenticate End-Users • Leverage trusted ID Provider to validate identity, credentials, and other attributes • End-Users access services quickly • Trustworthiness assured by GAIN Trustmark • Relying Parties can assess Identity Information Provider vs levels of assurance aligned to use cases and local regulations*
Relying Party Gains • Improved conversion • Efficient servicing processes • Effective account recovery • Minimal effort to integrate	Gain Creators • Minimal effort for End-Users to validate their identities improves conversion and efficiency • Recovery follows the same efficient process • 1 integration; interoperable Open Standards APIs
Relying Party Pains • Low conversion rate / high cart abandonment • Call centre calls for recovering user credentials • Costs to integrate - especially multiple systems • Costs to negotiate & manage multiple contracts • Costs to conduct full identity verification • Costs to comply with data protection regulation (when I store data myself) • Risks associated with inaccurate identities • Major capital investment • Unclear whether to trust identity data and attributes	Pain Relievers • Simple UX improves conversion rates • Financial institution app recovers login credentials • Single integration with global reach • Contract with global reach • Leverage financial institutions’ investment in KYC • Attributes are passed to - but do not have to be stored by - Relying Parties • Insurance as a value-added-service* • Transaction fee-based model reduces CAPEX • Identity Information Provider adhere to the GAIN Trust Framework

**These items are an extension of the initial GAIN launch: they are not planned for Day 1, and are not included in the forthcoming Blueprints.*

A.3 Identity Information Provider Value Proposition

Secure long-term relationships with your existing customers while transforming investments in customer identification, data security, and digital channels into a sustainable profit-centre with global reach.

Value for Financial Institutions means…	How GAIN Delivers
Jobs-to-be-Done • Maintain direct relationship with my customers • Profitable growth for my shareholders • Offer valuable services to my customers • Comply with regulation & legislation in my market • Ensure the security of customer transactions • Maintain my reputation for corporate responsibility	The Core Product & Services • Return on heavy investments in KYC and authentication, revenue & deepened relationships • Offers my customers seamless access to services • Flexes to architectures that meet local requirements • Ensure my customers' consent, privacy, and security • Leadership in building Digital Trust
Financial Institution Gains • Increased customer relevance • Increased returns on assets and investments • Global reach • Reduced costs and complexity - technology, legal, vendor relationships	Gain Creators • 100+ customer interactions per year • Leverage investment in KYC and digital technology • GAIN is interoperable across borders • Connect to 1 global system rather than disparate networks in jurisdictions around the world
Financial Institution Pains • Disintermediation • Complex operations • Inability to scale	Pain Relievers • Ensure direct 1-to-1 relationship with customers • 1 set of standards • Global identity and data standards can spur harmonized data regulations that facilitate scale* • Connect to 1 global system rather than disparate networks in jurisdictions around the world

Note: some of these value-drivers may not be relevant to all Identity Information Providers.

Appendix B - Business Model Outlines[27]

B.1 Financial Institutions

Financial Institutions may take on up to three roles: Identity Information Provider, Service Provider (onboarding Relying Parties), and as a Relying Party. This addresses the first two.

Value Propositions for B2C and B2B customers	***for End-Users*** (FI as Identity Information Provider): Use your trusted banking (or other financial Identity Information Provider) app to access almost anything online. ***for Relying Parties*** (FI as Service Provider): With GAIN, you can identify and authenticate your customers - wherever they are in the world - with a simple, high-trust experience. The UX is harmonized, similar to the global unified payment experience. This Increases conversion, while reducing the cost and complexity for Relying Parties.
Revenue Streams	***from End Users*** (as Identity Information Provider) ● A proportion of each chargeable identity verification transaction will flow to the Financial Institution as Identity Information Provider ● Indirect: More frequent interactions and deeper relationships with B2C customers ***from Relying Parties or GAIN*** (as data and service provider) ● Fixed fees to access the network ● Transaction fees ● Offering secondary services, e.g., insurance ● Indirect: Deeper relationships with B2B customers, brand recognition, and reputation for trust assurance
Key Partners	● GAIN operations ● Trust Networks in jurisdictions around the world ● Service providers (GAIN Members, Aggregators, etc.) who support in onboarding Relying Parties
Key Activities	Onboard and maintain GAIN connectivity and participation (Direct or via Service Providers)
Resources Required	Engineering capabilities to integrate the GAIN Technical Requirements Ongoing operation of the GAIN implementation 1st, 2nd, and 3rd line process & risk management 1st line customer support (End-User) Product Management
Cost Structure	Initial Implementation Ongoing Costs Membership Fees for GAIN governance and maintenance OPEX Potential additional costs for fulfilling additional requirements of the GAIN Service (p.ex. collecting additional data, fulfilling reporting obligations, ensuring higher requirements than those arising from own regulatory obligations)

B.2 Service Providers

Value Propositions for Relying Parties	***for Relying Parties*** (as Service Provider): With GAIN, you can identify and authenticate your customers - wherever they are in the world - with a simple, high-trust experience. Increase conversion; reduce the cost and complexity in your business.
Revenue Streams	Onboarding / Setup Fees Processing Fees A proportion of the revenue from each identity verification flows to Service Providers
Key Partners	GAIN (GAIN Operator and/or GAIN Board of Governors) Relying Parties
Key Activities	Onboard and maintain (legal) GAIN connectivity and participation Onboard Relying Parties Identification and Authentication of Relying Parties and adherence to the GAIN Rules Monitor Relying Parties’ adherence to the GAIN Rules and ensure enforceability of the GAIN Rules Billing and clearing of any fees to be paid to GAIN (or an Identity Information Provider)
Resources Required	Engineering capabilities to integrate the GAIN Technical Requirements at the Relying Party (if this service is offered). Ongoing monitoring of the Relying Party 1st line customer support (Relying Party) Product Management
Cost Structure	Initial Implementation Ongoing Costs Monitoring system Billing & Clearing system

B.3 GAIN (Operator and/or Board of Governors)

Value Propositions	***for End Users*** - as above (refer to Appendix A)
	for Relying Parties - as above (refer to Appendix A)
	for Trust Networks Connect your network to a global ecosystem - dramatically increasing your reach and, therefore, the value offered to relying parties and customers who transact around the world.
	for Financial Institutions as Identification Providers Turn a cost-center into a profit-center by leveraging existing capital-hungry assets (KYC and authentication processes; existing digital channels; security and privacy protections) to deliver high-trust identification solutions to a global marketplace.

Revenue Streams	Membership subscriptions / License fee (fix or transactional) for participation Data products and value-added services for the open market (e.g., insurance)
Key Partners	Identity Information Providers, including Trust Networks Service Providers Relying Parties (via Service Providers) (Qualified) Trust Services providers OpenID Foundation OIX
Key Activities	Build Governance structures Build & Maintain: ● Trust Framework ● B2B directory ● Test services ● Monitoring policies and processes ● Enforcement policies and processes ● Billing & Clearing
Resources Required	Capital (investors) to bridge until the GAIN break-even point People & Consultancy Services Outsourced services
Cost Structure	Initial Implementation ● Cost of the Proofs-of-Concept ● Consultancy Services ● Engineering Services ● Project Management Ongoing Costs ● People costs ● Outsourced services ● License fees to Identity Information Providers (as the case may be)

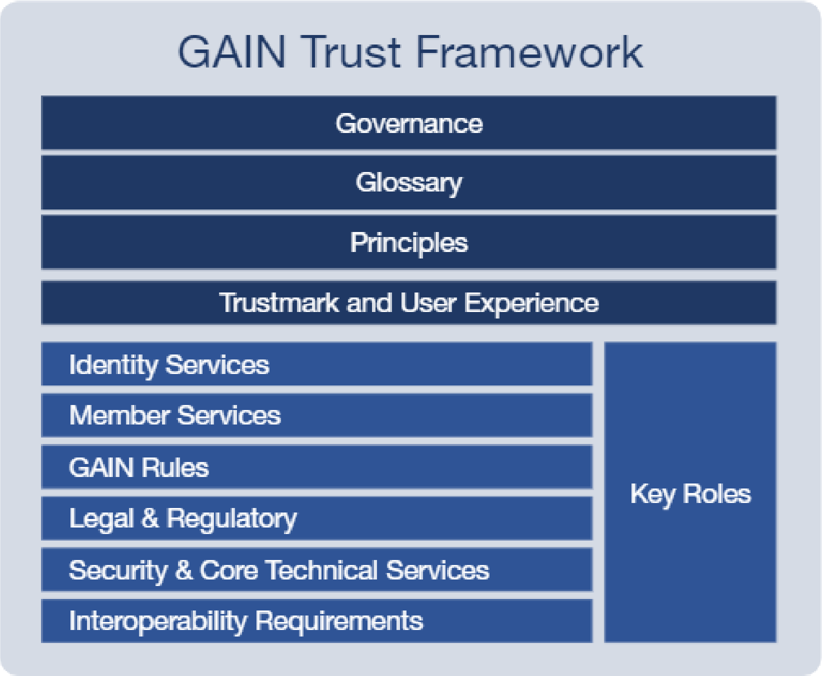
Appendix C - GAIN Trust Framework

Trust Frameworks lay out legally enforceable specifications and rules that govern a multi-party system. A GAIN Trust Framework will be established in order to ensure that:

1. End-Users can trust in the safety of data about them and the legitimacy of Relying Parties.
2. Relying Parties can use digital identity data with confidence.
3. All parties realize the benefits articulated in this paper.

The proposals herein are organised according to the best practices set out in the Open Identity Exchange's (OIX) 2017 guide[28] (see Figure C.1 below). As referenced in Figure 7 (above), working groups will convene to further develop this framework from now until early 2022.

Figure C.1 *- Contents of the GAIN Trust Framework*



Adapted from the OIX "Trust Frameworks for Identity Systems"

C.1 Glossary and Key Roles

Principle GAIN Actors	Definition
“GAIN Board of Governors”	the independent board that oversees the network and ensures that it successfully delivers targeted benefits to other parties in the network
“GAIN Operator”	the legal entity responsible for delivering the Core Technical Services (as defined below).
"End-User"	a natural person and the data subject wishing to have the Identity Information Provider share identity related data with a Relying Party.
“Identity”	set of attributes related to an entity [SOURCE] ISO/IEC 24760-1
“Identity Information”	set of values of attributes optionally with any associated metadata in an identity [SOURCE] ISO/IEC 24760-1
“Identity Information Provider”	an entity that makes available identity information [SOURCE] ISO/IEC 24760-1
“Relying Party”	organization that consumes Identity Services via the GAIN for the purpose of providing services to an End-User.
“Service Provider”	a legal entity that assists a Relying Party in participating in the GAIN (similar to an acquirer in a credit card scheme).
“GAIN Member”	any Identity Information Provider, Service provider or Relying Party that participates in GAIN.
“Trust Network”	An existing network or scheme, such as BankID Norway, BankID Sweden, Finnish Trust Network, iDIN, itsme®, NemID, yes®, etc., that connects an Identity Information Provider to the GAIN or acts as an Identity Information Provider itself. Such networks are also required to comply with the GAIN rules.

Note that a Relying Party is legally connected to GAIN via a Service Provider. In particular, the Service Provider signs up to GAIN and ensures, through suitable contractual arrangements, that the Relying Party (i) receives all relevant information for participating in the GAIN, and (ii) agrees to comply with the GAIN Rules. It is responsible for the Identification (as defined below) of the Relying Party in accordance with applicable regulatory requirements, which may vary depending on use case, region, etc. It will further ensure that the Relying Party fulfils the participation criteria (see "*GAIN Rules*") for the duration of its participation in the GAIN.

If a GAIN Member outsources technical services to a third party (such as a technical service provider), such third party shall act under the responsibility of the GAIN Member, e.g., outsourcing partner, data processor, etc. It will (in such a role) not have any contractual relationship with GAIN.

C.2 Governance, Principles, and Trustmark

To deliver the Trust Framework requires the oversight and management of a governing body. This paper proposes a “GAIN Board of Governors” responsible for maintaining and evolving the Trust Framework as required. This will include the definition of appropriate ‘checks and balances’ governing the system, including the governors themselves.

Table C.2: Proposed Principles Underlying the GAIN Trust Framework

Proposed Principle	GAIN Requirements
End-User Convenience	Adoption (by both End-Users and Relying Parties) will depend upon End-User convenience. The GAIN ecosystem ensures that End-Users interact with trusted Identity Information Providers, a familiar interface, and a simple process that connects them to services across the internet.
End-User Control and Choice	End-Users have control of their data. They may choose who they are shared with and how long for (purpose limitation). They also choose the Identity Information Provider involved. GAIN transactions are always initiated by End-Users.
Minimal Disclosure in view of Use Case & Recipients	Identity Information Providers share data directly with Relying Parties: Neither the GAIN nor any third party have access to End-User Data. Furthermore, Relying Parties can choose to request only the minimum required for their use case. End-Users will have control over whether to share each attribute.
Interoperability	*Technological Interoperability***:** The GAIN is designed to integrate with a variety of legacy infrastructures and identity solutions. See Appendix D for a deeper dive into technical interoperability. *Legal Interoperability:* The GAIN Rules will be codified in contracts that provide sufficient legal certainty as to participants’ duties and obligations and ensure enforceability. They will also facilitate liability risk allocations and assessments as needed. To ensure cross-border harmonization, these rules will be designed so as to minimize the applicability of certain existing legal and regulatory obligations in some jurisdictions.
Trust	A key to trust is the assurance that the relevant other parties are real, identifiable, and can be held accountable for their actions in the context of the GAIN. As such, authentication and identification are always required when interacting via GAIN - for any GAIN Member and End-User.
Ecosystem	GAIN sets the basis for an ecosystem by defining the “trust framework” or general “rules of the game” incl. standardized and harmonized legal (incl. Data Protection) and technical requirements (e.g., API standards). Within this trust framework, GAIN allows its participants to bring opportunities to the financial world, to work with new organizations and to provide to consumers new and innovative solutions. New compliance and governance measures are created to ensure that organizations can protect End User’s privacy and support End Users to get the value out of their data.

C.3 Trustmark & User Experience

A recognizable button or brand identifier (the GAIN brand is to be determined) will let End-Users know that they can initiate a transaction via a trusted environment where the GAIN Rules apply. This button will be positioned on the Relying Party's website, mobile application or other entry points.

The End-User will then choose their Identity Information Provider and authenticate via that Identity Information Providers' digital channel. If the End-User chooses a Trust Network, they will be directed accordingly, and any further steps will be defined by the standards of that Network.

The End-User will have an active role in any transaction and the process will take place within their trusted Identity Information Provider's environment. They request that the Identity Information Provider share relevant data with the Relying Party and the Identity Information Provider does so in execution of their contractual obligations (see also below under '*Data Protection*').

Note that GAIN establishes the link between the Identity Information Provider and the Relying Party based on the End-User's choice. However, End-User data is passed directly between Identity Information Provider and the Relying Party without passing through any GAIN components.

C.4 Identity Service

The following data should be available via the Identity Service:

- End-User Authentication level & methods, such as: Provider Login 1FA; Provider Login 2FA with phishing resistance based on EBA RTS on SCA[29].
- Digital Identity Data**,** such as: Email; Phone; Address; Given Name; Family Name; Place of Birth; Date of Birth; Nationalities.
- Verification and/or Validation Data and Attributes such as: Evidence used; date/time of data verification and validation; expression of various standardized LOA scoring; etc.

An Identity Information Provider must enable other GAIN Members, in particular Service Providers and Relying Parties, to rely on the result of the authentication procedures provided in the context of a GAIN Service. They must provide an End-User authentication method that complies with the applicable local legal and regulatory requirements. It will provide a Strong End-User Authentication if and to the extent required by law or the Relying Party. It must have appropriate security measures in place to protect the confidentiality and integrity of the personal data of the End-User.

The Identity Service (including End-User data) is exchanged directly between GAIN Members without the GAIN Operator or the GAIN Board of Governors coming into possession of the End-User data. Neither the service of transmission of data nor the data themselves originate from GAIN (or any GAIN entity) and therefore cannot be checked by GAIN (or any GAIN entity) for their legality, correctness and/or completeness.

A Relying Party that consumes the Identity Service, shall be obliged to use the obtained End-User data only for the intended purpose in accordance with the GAIN Rules and, in particular, shall not transfer the rights to such data to third parties unless such transfer takes place in accordance with the applicable statutory provisions (e.g., on order or with consent of the relevant beneficiary, generally the End User).

C.5 Member Services

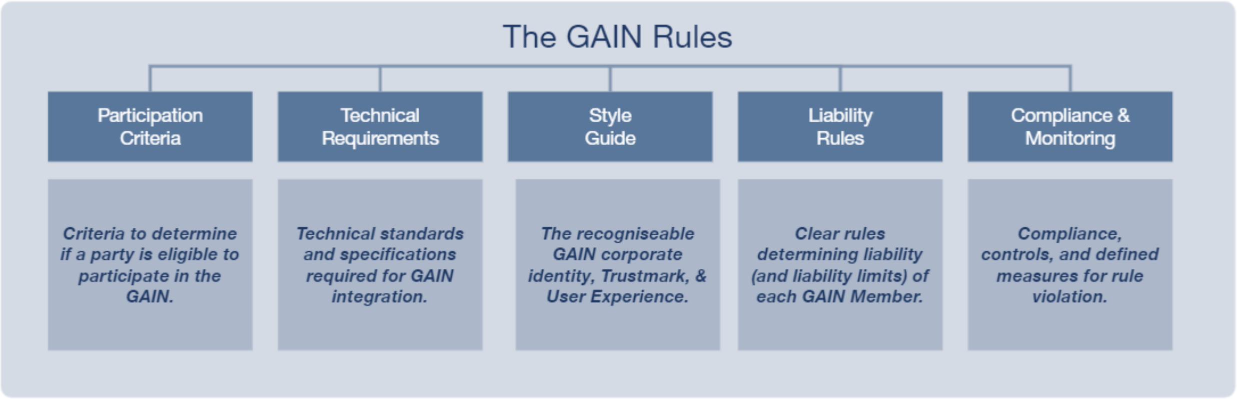
When on-boarding, GAIN Members will need to provide various details, and these will need to be verified to ensure that they are the entity they claim to be and that they fulfil the requirements to become a member of the network in whichever roles they request. Once this has been completed, they are able to begin transacting and are able to use Core Technical Services (see below under Core Technical Services) to ensure that they are interacting with other authorized GAIN Members.

Member Services will also allow on-going management of the service by GAIN Members, whether that is maintaining up-to-date information about the entity, managing fees, or withdrawing from the service.

C.6 GAIN Rules

The “**GAIN Rules**” are governed by the GAIN Board of Governors. The GAIN Rules are the general terms and conditions, applicable for any role, business and use case within GAIN. Being agreed on contractually, the GAIN Rules shall be applicable independently of the jurisdiction and applicable law of the GAIN Member. The GAIN rules may reflect statutory requirements for certain so-called “**Regions**”, such as Europe Region, United States Region, Middle East Region, Africa Region, Asia Region, etc.

Figure C.6: *The GAIN Rules*


The GAIN Rules
Participation Criteria
Technical Requirements
Style Guide
Liability Rules
Compliance & Monitoring
Criteria to determine if a party is eligible to participate in the GAIN.
Technical standards and specifications required for GAIN integration.
The recogniseable GAIN corporate identity, Trustmark, & User Experience.
Clear rules determining liability (and liability limits) of each GAIN Member.
Compliance, controls, and defined measures for rule violation.

C.7 Participation Fundamentals

In order to participate in the GAIN, each GAIN Member must be identified and authenticate itself (the "**Identification**"). The level of identification depends on the GAIN Services provided or consumed. The consummation of certain GAIN Services may require the verification and validation of the business identity of the GAIN Member in accordance with applicable regulatory requirements, such as AML, eIDAS or other regulatory requirements.

The GAIN will be organized as a license model (similar to a credit card scheme), i.e., a GAIN Member receives from the GAIN Board of Governors a license to participate in the GAIN and to provide or procure GAIN Services. Further, licenses may be granted, e.g., to use certain components provided by the GAIN, which enable a GAIN Member to establish a connection to other GAIN Members for the exchange of GAIN Services, incl. service configurations, directories etc., to implement APIs according to the technical requirements of the GAIN or to use relevant IP, trademarks etc. necessary for the participation in GAIN.

Potential GAIN Members may onboard via a standardized onboarding process where they accept the GAIN Rules and identify according to the requirements of the role they take within the network and/or the relevant GAIN Services they intend to offer or consume.

C.8 Technical Fundamentals

The GAIN will provide a sandbox for testing purposes. Any technical integration, including changes to an existing integration or additions to a new integration (e.g., in the case of new GAIN Services) shall be tested in such sandbox before activation.

Core Technology Services are the subject of Appendix D.

C.9 Monitoring and Compliance Fundamentals

To maintain trust, compliance with the GAIN Rules will be monitored. Defined evidence of compliance and controls should be presented on a periodic basis and on request. Wherever possible, monitoring will be automated, this will be appropriate for verifying conformance to technical specifications and delivery of performance and availability requirements. Verification of compliance with other GAIN policies will be monitored through the use of periodic audits with reporting of status in a structured fashion. Key data points derived from the monitoring regimen will be made available to all members of the network.

If a GAIN Member does not comply with the GAIN Rules, it is the role of GAIN to take actions and, as the case may be, sanction such a GAIN Member. Such sanction measures may be:

- warning of the GAIN Member;
- restriction of the GAIN Member's rights under the GAIN Rules;
- revocation of the GAIN Member's special status (e.g., as Identity Information Provider or Relying Party);
- temporary blocking of the GAIN Member;
- partial or even complete withdrawal of the GAIN Member’s rights under these GAIN Rules;
- definite blocking of the GAIN Member.

C.10 Salient Legal Aspects

C.10.1 Liability

Liability risk is a key concern for all participants in GAIN, regardless of their role (Identity Information Provider, Relying Party, GAIN Operator, GAIN Board of Governors, etc.), although the extent of such risk will vary by role. Generally, a participant in GAIN can be liable (i.e., legally responsible for paying damages to compensate others, including nonparticipants) whenever that participant is in some way “at fault” or “responsible” for a loss suffered by someone else. This occurs whenever a participant breaches a legal duty it owes to someone else to act (or to refrain from acting) in a certain way, thereby causing the loss.

Those legal duties, that can be used to form the basis of a participant’s liability, come from three sources:

1. Existing general law in each applicable country with jurisdiction over the transaction (e.g., contract law, privacy/data protection law, tort law, antitrust/competition law, tax law, banking law, etc.);
2. New/developing identity system law, if any, enacted in each applicable jurisdiction to specifically govern identity systems generally (e.g., the Virginia Identity Management Act, the draft UNCITRAL identity management rules, etc.); and
3. Contract-based system rules developed to govern the participants in an operation of GAIN (e.g., often referred to as a trust framework, scheme rules, operating rules, governing rules, etc.).

The first two sources of these legal duties are statutory or regulatory, will likely vary from one country to another, and are largely outside the control of GAIN. Laws governing privacy/data protection, consumer protection, and limitations on certain damages (e.g., that you cannot disclaim damages involving personal injury) typically fall into this category. Thus, participants in GAIN will be subject to whatever liability risks are imposed by these two sources of legal duties.

However, in many cases, other legal duties imposed by law or regulation can be modified or supplemented by the third source of legal duties – i.e., by contract-based system rules to which all participants agree to be bound. The GAIN Rules will be that contract-based set of system rules that will govern GAIN, will be unique to GAIN, will seek to clearly define the duties/obligations of each participant in GAIN, and will allocate the liability risk between and among them.

Because the GAIN Rules govern the operation of the network, they provide a vehicle to structure the network in a manner designed to minimize the applicability of some existing law (e.g., by avoiding activities subject to regulation). At the same time, by defining the legal duties imposed on each participant role (which, of course, will be a key source of liability if breached), the GAIN Rules will provide a fair degree of legal certainty as to the duties imposed on each participant role, and facilitate liability risk allocations and assessments as needed. Further, in the event a legal duty is breached by a participant, the GAIN Rules can be used to allocate liability among the participants involved (e.g., through exclusions or limitations on liability, if appropriate) in a manner that works best for that network.

Of course, all participants in the network would prefer a total exclusion of all of their liability risk. But as a practical matter, liability is a zero-sum game. That is, if someone suffers a loss, if the liability of the participant whose breach of duty caused the loss is excluded or limited, that doesn’t eliminate the loss, it merely shifts the loss on to someone else. Thus, the GAIN Rules will be the vehicle by which liability risk is allocated and equitably shared among the relevant participants.

C.10.2 Data Protection & Policy

The End User shall always stay in control over personal data about them. To achieve this, any transfer of the aforementioned data shall only be initiated by its explicit choice, i.e., on order of the End User itself. Due to this, the necessity of consents and the complications which arise from them - e.g., by terms of the GDPR - could be omitted. Instead, any transfer of data is performed as an action for performance of contractual obligations without the need of any data protection consent.

Neither the GAIN Board of Governors nor the GAIN Operator will process or persist any personal data of End Users at all. Instead, any personal data transfer will take place directly between the GAIN Members. By doing this, on one hand it is possible for each GAIN Member to act on their own responsibility in terms of data protection, i.e., each GAIN Member is individually responsible for fulfilling its own data protection related regulatory requirements towards the End User, such as properly informing the End User on its privacy policy.

Further, the need for data processing agreements and pitfalls like shared or undefined responsibilities will be avoided. On the other hand, it helps to keep the End User in full control of its personal data, as such data is only shared between the relevant parties without involving third parties in the data transfer.

Finally, it also avoids the risk of the GAIN Board of Governors or the GAIN Operator posing a threat to the GAIN Members, e.g., by collecting End User data enabling them, at some point, to provide the Identity Service itself.

Due to the fact that each GAIN Member acts on its own responsibility in terms of data protection and is regulated by different supervisory agencies, it is crucial that GAIN establishes a framework, which enables GAIN Members to choose in which regions or countries they decide to act and which level of data protection they intent to provide or consume (e.g., GDPR, LGPD, etc.). For example, an Identity Information Provider or Relying Party submitted to the GDPR wants to exclude all regions and countries from interaction which are not under jurisdiction of the GDPR or are not determined by the European Commission to ensure an adequate level of protection by reason of their domestic law or of the international commitments they have entered into. In consequence, a foundation for the differentiable international usage of personal data and corresponding services could be built on a regulatory sound basis, including requirements for a high protection level for personal data. This is necessary as GAIN is a trust network which cannot afford to lose the trust of any of its involved parties due to an insufficient protection of personal End User data.

C.10.3 Regulatory Framework(s) & Requirements

For GAIN to operate globally, it is crucial that GAIN itself avoids providing any regulated services. While GAIN Members may provide to the End User regulated services within their pre-existing licenses, the GAIN cannot provide any of such services – otherwise, GAIN would lose its flexibility in operating globally.

Since GAIN plans to operate outside the scope of the current regulatory landscape, it is important to design its services in such a way that the regulatory scope of national and international laws is not applicable. Money remittance businesses, payment initiation services (PIS) and account information services (AIS) are typically subject to banking, financial or payment services regulation requiring such license. GAIN will therefore avoid providing these regulated services.

Stepping outside of regulations, GAIN needs to clearly define its role within the ecosystem. As already mentioned throughout this Whitepaper, GAIN will to take the position of rule/standard setting entity without involvement (other than, as the case may be, enablement of technical transmission) in the services provided by GAIN Members.

C.10.3.1 Regulation of billing and clearing

It is important that GAIN Members can be remunerated for their services without the GAIN being required to obtain a license or be subject to additional regulations. Billing and clearing of the claims between the GAIN Members needs to be implemented within the GAIN Rules. Money remittance businesses, however, are a regulated activity in many jurisdictions (e.g., as payment service under European PSD2 or with regard to AML/CTF law in Australia).

Typically, the regulatory frameworks on money remittance regulate a transfer of funds as intermediary. In many jurisdictions, it is not required that a bank account is maintained but the regulation captures traditional money transfer companies as well as modern platform businesses taking care of the payment process.

GAIN will be organized as a license model (see also above under *GAIN Rules*). This will inter alia allow GAIN to stay in the payment flow and at the same time avoid any regulation in relation to the transfer of funds (i.e., money remittance business).

C.10.3.2 Regulated services of GAIN Members

GAIN Members holding sufficient licenses or regulatory approval can provide their regulated services to the End User. In those cases, it must be clear that the GAIN Member is responsible for obtaining and maintaining such license and that the GAIN Member is the only one responsible for complying with any regulatory obligation. There must be a provision in the GAIN Rules that the GAIN Members are not allowed to provide regulated services via the scheme if not holding relevant licenses.

If GAIN wants to implement certain services via its scheme by assigning certain roles, it should limit its involvement to technical services as a maximum. Banks and other regulated entities may wish to provide various services (e.g., account information services and payment initiation services) using GAIN. While it might be possible to communicate such capabilities via the GAIN, it will only be enabled in a way that does not result in additional regulation or requirement for licensing for GAIN itself.

C.10.4 Interoperability Requirements

The intention of GAIN is that it provides interoperability across jurisdictions and industry verticals and relying parties will be able to use the digital identity data to enhance their user propositions. Interoperability is one of the primary enablers that GAIN will deliver. It allows parties from across the network to easily connect with one another and understand the context within which the data is provided.

There are three pertinent domains of interoperability that are all needed within GAIN for the full benefit to be realised and for members to readily use the data available:

C.10.4.1 Policy and Procedure

When relying upon digital identity data it is necessary to have an understanding of the context within which it was collected, maintained and provided. The policies and procedures that are applied by a provider are of interest to a relying party because they allow the relying party to be assured that the digital identity data is of a level that is (or is not) adequate for their purposes and whether it fits within the local regulatory requirements. Aligning and being able to communicate the policies that were applied adds important context to the digital identity data provided. Examples of this might be details of the legal requirements that were used when collecting identity data or how identity verification is performed by a specific provider and the level of assurance score that was assigned to the digital identity by the provider (e.g., a digital identity may be proofed under NIST SP 800-63A).

C.10.4.2 Data and Metadata

When data and metadata are exchanged between parties it is important that they are properly understood by the relying party and that they are consistent across providers. Attribute names and meanings need to be standardized in order that relying parties can integrate provided attributes with their use cases.

C.10.4.3 Protocol

Interoperability at a protocol layer is required to deliver a service that is easily and cheaply integrated for relying parties resulting in greater appetite for the use of GAIN and a quicker time to value for all parties involved. The details of the protocol interoperability will be discussed further in the Architecture blueprint.

As part of the GAIN rules providers will be expected to meet standards for interoperability, performance and availability in order that an effective interoperable network is maintained. As part of GAIN membership there will be a requirement for monitoring of conformance to those standards. The required monitoring will use automated mechanisms wherever possible and will be delivered as one of the GAIN core technical services. Where automated monitoring is not possible periodic audits will be required.

C.11 Core Technical Services

GAIN provides each GAIN Member with various components that enable the GAIN Member to establish a secure connection via GAIN (collectively, the “Core Technical Services”; cf. also the relevant Technical Requirements). Further details of these services are expressed in Appendix D.

Appendix D - Draft Technical Architecture

D.1 Overview

This Appendix describes the draft technical architecture of the GAIN and comprises of

- Stakeholders List;
- Stakeholder concerns and its mapping to architecture views; and
- Architecture views.

“Stakeholder concerns” are the drivers of value that the architecture should address for different actors in the ecosystem. An Architecture View expresses the Architecture of the GAIN from the perspective of one or more Stakeholders to address specific concerns. They are addressed by at least one architecture view (Table D.1).

D.2 Stakeholder Concerns of the GAIN

In GAIN, there are five principal stakeholders:

1. End-User,
2. Relying Party,
3. Identity Information Provider,
4. Service Provider, and
5. GAIN Entity.

In addition to those principal stakeholders, GAIN recognize the following as important stakeholders:

- Civil Society
- Regulators
- Investigators and Prosecutors

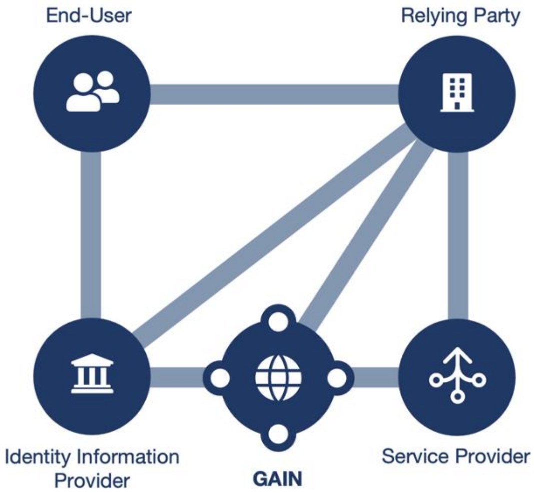


Table D.1 outlines the stakeholder concerns derived from the source of the benefits articulated in this document. The remainder of Appendix D will provide ‘views’ in which those concerns are addressed. Note: as working groups and proofs-of-concept continue, more requirements and nuances will be identified.

Table D.1: Projected Concerns of the Principal Stakeholder

Stakeholder	Stakeholder Concerns	Corresponding Views
End-User	Secure way to share data	Data Flow View
	Simple, convenient experience	End-User Experience View
	Selective control over what data is shared	End-User Experience View & Data Flow View
	Trust in the legitimacy of Relying Parties	Operations View & Data Flow View
Relying Parties	Securely access End-User identity data and services	Data Flow View
	Ability to evaluate the level-of-trust for any given attribute	Data Flow View
	Broad reach of End-Users without requiring a contract with individual Identity Information Providers	Operations View & Data Flow View
	Simple, uniform End-User experience to optimise conversion and servicing efficiency	End-User Experience View
Identity information Providers	Better service to its customers providing assured space to transact	End-User Experience View
	Flexibility to implement a solution that aligns with goals and local context	Data Flow View
GAIN	Transparent information about ● when and how Relying Parties were on-boarded ● when Relying Party keys were registered and retired ● when the attribute Provider keys were registered and retired	Data Flow View
	Controlled onboarding of Relying Parties Provide Identity Information Provider Chooser	End-User Experience View
Service Providers	Streamlined integration	Data Flow View
	Customer support	
	Flexibility to implement a solution that aligns with goals and local context	

D.3 Architecture Views

D.3.1 Overview

This section explains various aspects of the GAIN architecture through the following views:

- End-User Experience View
- Data Flow View
- Operations View
- Privacy View

Each view addresses some of the concerns expressed in the Table D.1. It should also be noted that each concern may be addressed by multiple views.

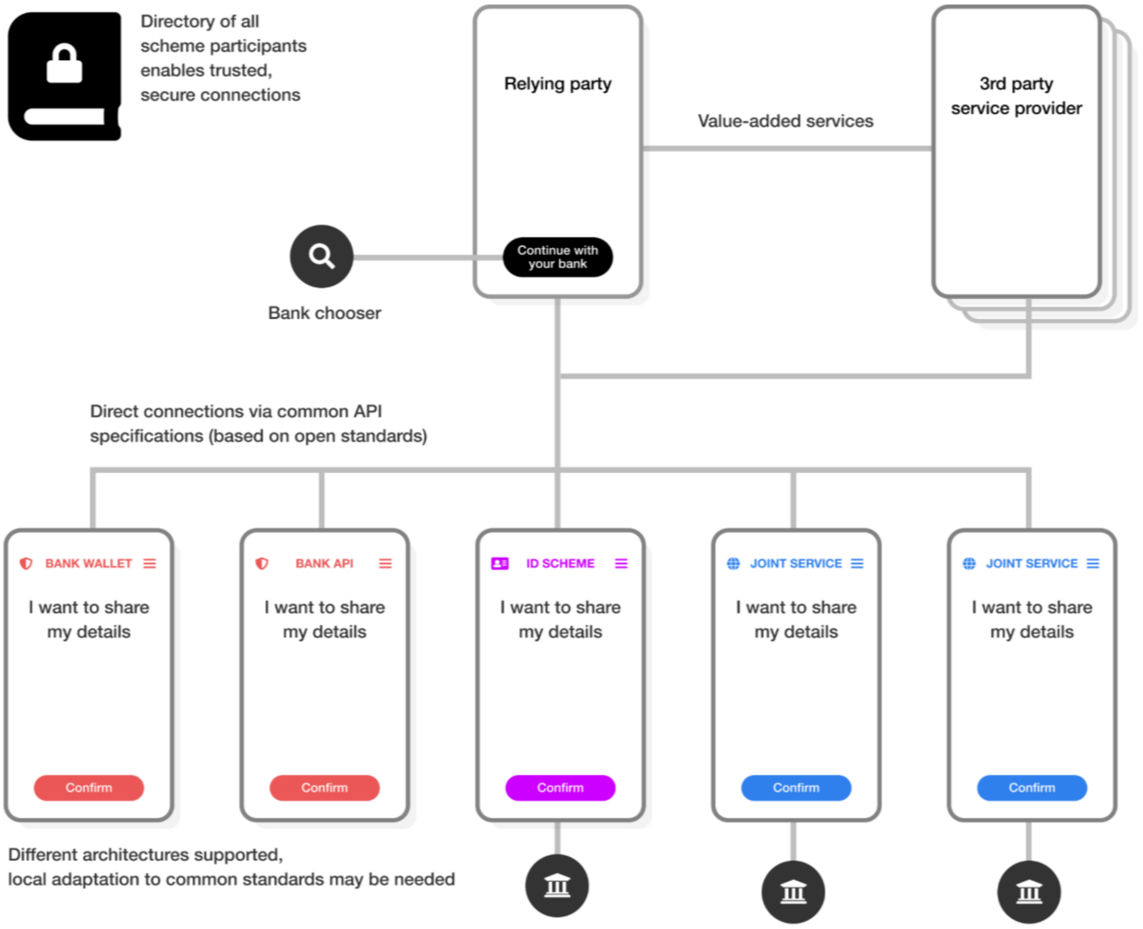
D.3.2 End-User Experience View

End-Users in GAIN will enjoy the use of the Identity Information Provider of their choice in GAIN rather than being forced to create accounts at each Relying Party. Using their chosen Identity Information Provider, the End-User will be able to share attributes selectively, present assured attributes, and monitor where their data is shared to and for what purposes.

D.3.2.1 Identity Information Provider Chooser

Leveraging the Identity Information Provider Metadata Directory, Relying Parties can provide a user interface from which the End-User can choose their desired Identity Information Provider.

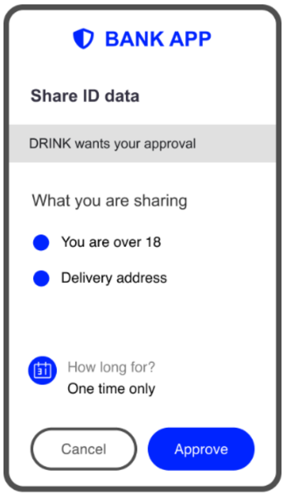
Figure D.2: The Identity Information Provider Chooser allows an End-User to search and pick their Identity Information Provider at the Relying Party


Directory of all
scheme participants
enables trusted,
secure connections
Relying party
Continue with your bank
Value-added services
3rd party service provider
Bank chooser
Direct connections via common API specifications (based on open standards)
BANK WALLET
BANK API
ID SCHEME
JOINT SERVICE
JOINT SERVICE
I want to share my details
I want to share my details
I want to share my details
I want to share my details
I want to share my details
Confirm
Confirm
Confirm
Confirm
Confirm
Different architectures supported,
local adaptation to common standards may be needed

The Relying Party will remember which Identity Information Provider the user has selected so that subsequent visits by the End-User can skip the Identity Information Provider filtering and can directly choose the preferred Identity Information Provider.

D.3.2.2 Selective Data Sharing

In the GAIN, Relying Parties are expected to adhere to the principle of collection limitation and purpose limitation. RPs will utilize the fine-grained attribute request capability of OpenID Connect to only collect the attributes needed for the purpose. The purpose will be presented to the End-User as recommended by ISO/IEC 29184 Online notice and consent (2020) using a layered approach.


BANK APP

Share ID data

DRINK wants your approval

What you are sharing

● You are over 18

● Delivery address

How long for?
One time only

Figure D.3: Selective attribute sharing

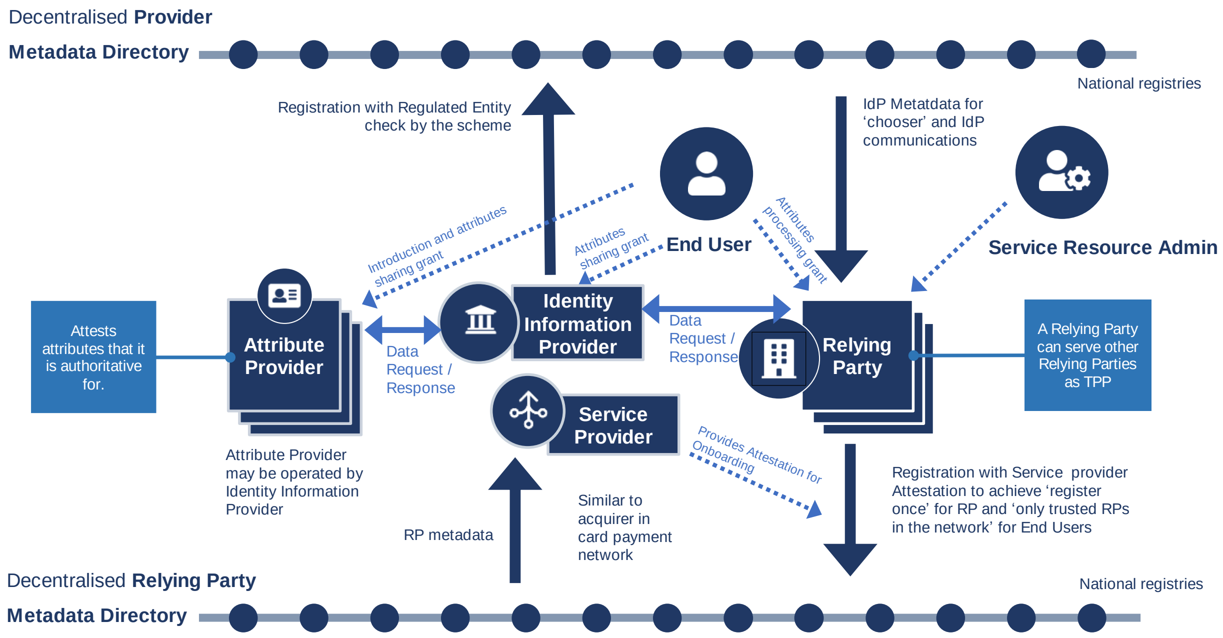
D.3.2.3 Privacy Dashboard

Participating Identity Information Provider in GAIN will provide a dashboard from which the End-Users can find out easily where and which data has and is being shared for what purpose and how. End-Users can review where data has been shared and stop any persistent sharing from within the Identity Information Provider Dashboard.

D.3.3 Data Flow View

Data Flow View provides how the Information including user and administrator direction flows and stored among the roles to be implemented in GAIN.

Figure D.4: Data Flow in the GAIN



Decentralised Provider
Metadata Directory
National registries
Registration with Regulated Entity check by the scheme
IdP Metatdata for 'chooser' and IdP communications
Introduction and attributes sharing grant
Attributes sharing grant
End User
Attributes processing grant
Service Resource Admin
Attests attributes that it is authoritative for.
Attribute Provider
Data Request / Response
Identity Information Provider
Data Request / Response
Relying Party
A Relying Party can serve other Relying Parties as TPP
Service Provider
Provides Attestation for Onboarding
Attribute Provider may be operated by Identity Information Provider
RP metadata
Similar to acquirer in card payment network
Registration with Service provider Attestation to achieve 'register once' for RP and 'only trusted RPs in the network' for End Users
Decentralised Relying Party
Metadata Directory
National registries

Note: RP Onboarding requirements may differ from jurisdiction to jurisdiction and it probably requires multiple levels of identity proofing and verification.

- **End-User:** End-User is a role primarily performed by individuals and is the central role in the GAIN. They are authenticated by User-AuthN and control how and where their data is being shared and used.
- **Service Provider:** It is a role that performs initial authentication (identity proofing) of the Relying Party and provides standardized attestation which Relying Parties can take and provide to the Relying Party Metadata Directory. This role is typically played by a regulated entity that has a requirement for identity proofing of the Relying Parties as their customer. It
  - implements the management system to achieve the assurance level expressed in the attestation;
  - support mapping of the Relying Party to a Legal Entity Identifier (LEI)[30] and a verifiable LEI (vLEI)[31] in partnership with the Global Legal Entity Identifier Foundation (GLEIF)[32]; and
  - support issuing the attestation in the standard format adopted by GAIN that include the information above.

- **Identity Information Provider:** This role authenticates the End-User, enables End-User to selectively share their data with the Relying Party along with the End-User Authentication result. The data shared may be locally sourced or collected from external Attribute Providers. This role is sometimes called “Consent Manager”. This role
    - supports Secure Customer Authentication;
    - provides information about level of assurance and the trust framework used;
    - provides data in the form Aggregated or Distributed Claims or as a verifiable presentation;
    - Communicates information via either ID Token or UserInfo endpoint (in the first standard interface)
    - supports Grant Management to allow Relying Parties to manage individual grants; and
    - provides a dashboard on where and what data was shared to End Users.
- **Attribute Provider**: It is a role that provides attested End User attributes at a certain level of assurance. This role could be played by an Identity Information Provider or an independent party. The attestation
    - supports proof that enables the receiving party to verify the provenance and assurance level of the contained data as well as whether the attestation was tampered or not. Format envisioned to be used in this respect is JWT as in OpenID Connect and W3C Verifiable Credentials.
- **Relying Party:** Is a role that relies on the End-User authentication result (Authenticated Identity, e.g., ID Token) and other data provided by the Identity Information Provider and Attributes provider roles. It typically serves End-User by utilizing the data but it can serve other entities and might not have direct interactions with End-Users. Relying Parties
    - implement Dynamic Client Registration to register to the Relying Party Metadata Directory using Attestations provided by its Service Provider;
    - implement OpenID Connect for Identity Assurance to receive Authenticated Identity to receive data; and
    - Implement OAuth Grant Management to request fine grained authorization.
- **Service Resource Admin:** It is a role that manages the access to the resource at the corresponding Relying Party. Its decision depends on multiple factors including but not limited to the payment status by the End User.
    - **Provider Metadata Directory:** It manages the metadata such as keys and endpoints of Identity Information Providers, Attribute Providers, and Service Providers in GAIN. It will also maintain when the Provider keys were registered and retired. It will maintain the historical data as well. The data contained in it will be used for Identity Information Provider Discovery and Chooser.
- **Relying Party Metadata Directory:** It manages the metadata such as keys and endpoints of Relying Parties in GAIN. It supports Dynamic Client Registration coupled with Attestation from the RP-AuthN role. It will provide
    - when and how Relying Parties were on-boarded and
    - when Relying Party keys were registered and retired as well.

  The data is used for RP Discovery and makes it possible for an RP to register only once to the network and be identified by all the Identity Information Provider in GAIN.

D.3.4 Operation View

GAIN will complement the existing and future financial services as needed, e.g., it will provide trust management, Registration, Discovery, Trust Management, Support, and (optionally) Billing (optional), and as well as Analytics Support.

- **Registration:** the GAIN provides new members a single registration interface with one or more processes for establishing the validity of the applicant organization. Options that will be elaborated in the design will include using attestation from the organization’s banking provider and, in partnership with the Global Legal Identifier Foundation (GLEIF)[33] use of the Legal Entity Identifier (LEI)[34] and the emerging verifiable LEI (vLEI)[35]. By registering just once with a strongly assured organizational identity the registration service will enable access to every Identity Information Provider in GAIN. The same applies to the client (RP) registration, this time with its own attestation.

- **Discovery:** the GAIN provides bank selection and discovery functions for technical details (e.g., endpoints). Authorization and access to APIs is performed directly between the recipient and the respective service provider. The user will see a Identity Information Provider selector dialog, when engaging in an identity transaction, as depicted in the screens in chapter 2. It is also planned that RPs will be able to request a filtered list of Identity Information Provider based on some conditions such as geography, jurisdiction, or capability.
- **Trust Management:** the GAIN provides the necessary functions to enable participants to establish secure connections by way of provisioning of technical details to the scheme participants, e.g., recipients are provided with the endpoints of the Identity Information Provider and all registered enterprises are provided with the technical details required to identify, authenticate and authorize each other. This is supported by a process of verifying and monitoring the status of GAIN members to ensure their on-going compliance with network rules and responsibilities.
- **Monitoring and testing:** Interoperability among the different deployments in the scheme is achieved via effective delivery of standardized APIs and protocols. Conformity to the respective standard will be tested periodically. Availability and performance will also be monitored to ensure the agreed thresholds are met and that effectiveness of the network is not compromised.
- **Risk information sharing and coordination:** The scheme provides a uniform interface to share attack and compromise information in real-time.
- **Support:** The scheme defined the support model for end-users, relying parties and Identity Information Providers.
- **Dispute resolution:** In the case of dispute, the concerned party may invoke a dispute resolution process via GAIN. This may include re-identification of the party that was anonymous or pseudonymous to the concerned party or some liability being taken by the provider
- **Billing:** Optionally the service providers can utilize the scheme as a billing engine by providing records about provided data and successfully performing service requests to the scheme as a basis for invoicing and settlement.
- **Analytics:** improving the performance of the scheme requires deep understanding or usage patterns across all participants of a certain use case. Optionally the scheme could collect and distribute analytical data among the scheme participants in order to facilitate this process.
- **Integration:** For existing deployments, there is the option to build an adaptation layer to bridge existing service implementations to the common technical interface. Building an adaptor for a specific deployment allows for flexibility that takes into account the design and capabilities of the respective deployment.

D.3.5 Privacy View

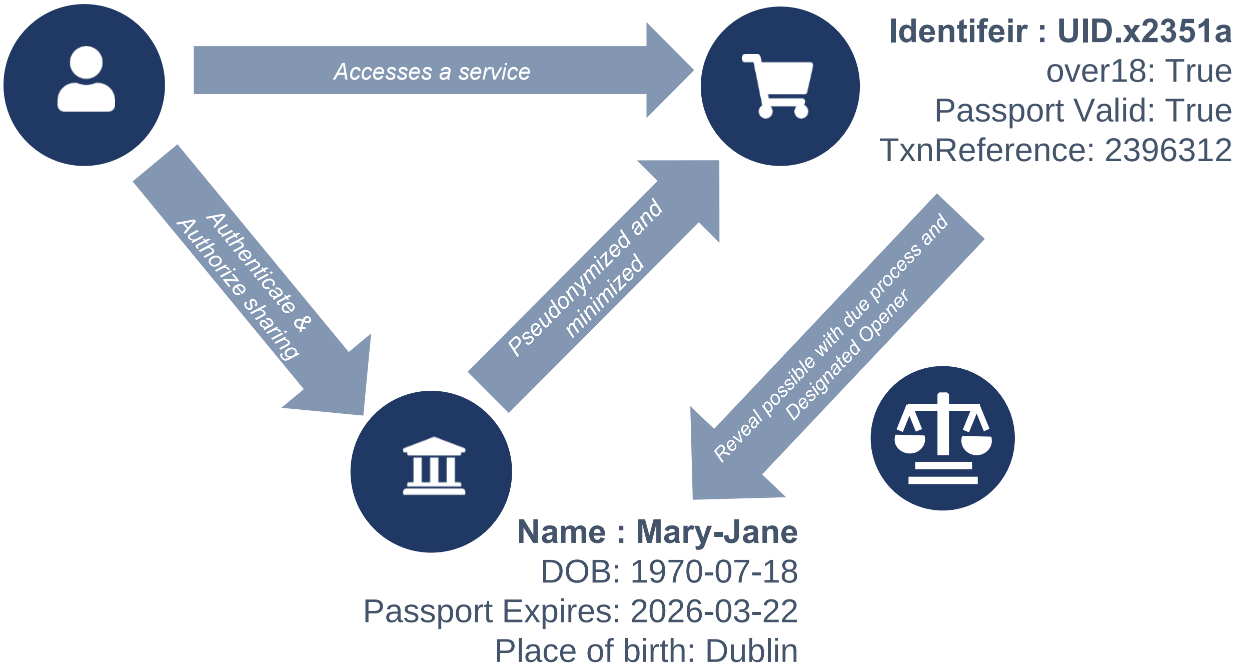
End-User privacy is protected through multiple layers of measures in GAIN. In this document, we will just point out some notable features.

D.3.5.1 Partial Anonymity and Pseudonymity

Although all the End-Users have been through some level of identity verification, creating an assured identity, it does not mean that End-Users must always be broadly identifiable. In day-to-day transactions, the principle of minimum disclosure will be followed and End-Users can remain anonymous or use pseudonymous with the Relying Parties and Services if the use case allows.

However, in the GAIN, when there is a dispute or evidence of criminal activity, there will be a process to link the anonymous or pseudonymous transactions to the End-User by a special entity called ‘Designated Opener.’ The concept is defined in ISO/IEC 29191 Requirements for partially anonymous, partially unlink-able authentication.

Figure D.5: De-anonymisation in GAIN



Disclaimer

This paper represents a collaborative effort among professionals within the identity space to author a White Paper highlighting the unique opportunity the global financial services sector can play in catalysing a collaborative solution to society's digital trust challenges However, statements made in this paper do not necessarily reflect the personal view of each contributor or that of their respective employer and/or client(s).

References

[1] European Monitoring Centre for Drugs and Drug Addiction (2016), The internet and drug markets, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg https://www.ofdt.fr/BDD/publications/docs/Insights21InternetDrugMarkets160211.pdf.

[2] Burt, A. (2019) Privacy and Cybersecurity are Converging: Here's why that matters for people and companies. *Harvard Business Review* https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

[3] McKinsey Global Institute (2019) *Digital identification: A key to inclusive growth.* [Accessed 12 July 2021] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf

[4] Spadafora, A. (2020) *Struggling with password overload? You're not alone* https://www.techradar.com/news/most-people-have-25-more-passwords-than-at-the-start-of-the-pandemic

[5] World Economic Forum (2018) *Identity in a Digital World: A new chapter in the social contract.* [Accessed September 8 2021] http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

[6] United Nations Office on Drug and Crime, *Money Laundering Overview* [Accessed 24 August 2021] https://www.unodc.org/unodc/en/money-laundering/overview.html.

[7] The World Bank, IBRD-IDA, *GDP (current US$)* [Accessed 24 August 2021] https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

[8] 116th Congress (2019-2020) *H.R.8215 - Improving Digital Identity Act of 2020* [Accessed 19 August 2021] https://www.congress.gov/bill/116th-congress/house-bill/8215/text?r=20&s=1.

[9] Monetary Authority of Singapore (2021) *Foundational Digital Infrastructures for Inclusive Digital Economies* [Accessed 15 August 2021]

https://www.mas.gov.sg/-/media/MAS/Fintech/FDI/Foundational%20Digital%20Infrastructures%20for%20Inclusive%20Digital%20Economies.pdf

[10] ID2020 (2020) *ID2020 At A Glance* [Accessed 18 August 2021] https://id2020.org/uploads/files/ID2020-Alliance-Overview.pdf.

[11] World Economic Forum (2018) *Identity in a Digital World - A new chapter in the social contract*, September 2018 [Accessed 7 July 2021] http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

[12] McKinsey Global Institute (2019) *Digital identification: A key to inclusive growth.* [Accessed 12 July 2021] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf

[13] Security Magazine (2017) *Average Business User has 191 Passwords* [Accessed on 5 September 2021] https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

[14] Burt, A. (2019) Privacy and Cybersecurity are Converging: Here's why that matters for people and companies. *Harvard Business Review* https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

[15] World Economic Forum (2018) *Identity in a Digital World - A new chapter in the social contract*, September 2018 http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

[16] Institute of International Finance (2020) *Digital Identities in Financial Services - Part 3: The Business Opportunity for Digital Identity* [Accessed 5 July 2021] https://www.iif.com/Portals/0/Files/content/Innovation/03_06_2020_%20difs.pdf

[17] McKinsey & Company (2020) *A test of resilience: Banking through the crisis, and beyond, McKinsey Global Banking Annual Review 2020* [Accessed 12 July 2021] https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/mckinsey%20global%20banking%20annual%20review%202020%20a%20test%20of%20resilience/a-test-of-resilience-banking-through-the-crisis-and-beyond-vf.pdf?shouldIndex=false

[18] Institute of International Finance (2020) *Realizing the Digital Promise: Part 1* [Accessed 5 July 2021] https://www.iif.com/Portals/0/Files/content/Innovation/02_19_2020_digital_promise.pdf.

[19] McKinsey Global Institute (2019) *Digital identification: A key to inclusive growth.* [Accessed 12 July 2021] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf

[20] Gallaun, G. (2021) *Case Study: How eIDs make proving your identity easier, faster, and almost free*, Wise, 18 August 2021 [Accessed on 23 August 2021] https://wise.com/gb/blog/how-eids-make-proving-your-identity-easier-faster-and-almost-free?&utm_medium=organic_social&utm_source=Linkedin&utm_campaign=All&utm_content=44429_eID

[21] World Economic Forum (2016) *A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity* [Accessed on 5 July 2021] http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

[22] Birch, D. (2014) *Identity is the New Money*. London Publishing Partnership: London

[23] Citibank N.A., (2019) *The Age of Consent - The Case for Federated Bank ID* [Accessed on 5 July 2021] https://www.citibank.com/tts/sa/flippingbook/2019/the-age-of-consent/gra30727_TTS_age_of_consent/20/.

[24] McKinsey Global Institute (2019) *Digital identification: A key to inclusive growth.* [Accessed 12 July 2021] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf

[25] https://www.cbinsights.com/research/fintech-smart-money-vc-digital-id-investments/

[26] Strategyzer *Value Proposition Canvas* [Accessed 15 July 2021] https://www.strategyzer.com/canvas

[27] Strategyzer *Business Model Canvas* [Accessed 15 July 2021] https://www.strategyzer.com/canvas

[28] Open Identity Exchange (2020) *A Guide to Trust Frameworks and Interoperability* https://openidentityexchange.org/guide-trust-frameworks-interoperability

[29] European Banking Authority *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2*

https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

[30] Global Legal Entity Identifier Foundation *Introducing the Legal Entity Identifier (LEI)* [Accessed on 9 September 2021]
https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

[31]Global Legal Entity Identifier Foundation *Introducing the Verifiable LEI (vLEI)* [Accessed on 9 September 2021]
https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/introducing-the-verifiable-lei-vlei

[32] Global Legal Entity Identifier Foundation *GLEIF – Global Legal Entity Identifier Foundation* [Accessed on 9 September 2021]
https://www.gleif.org/

[33] Global Legal Entity Identifier Foundation *GLEIF – Global Legal Entity Identifier Foundation* [Accessed on 9 September 2021]
https://www.gleif.org/

[34] Global Legal Entity Identifier Foundation *Introducing the Legal Entity Identifier (LEI)* [Accessed on 9 September 2021]
https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

[35] Global Legal Entity Identifier Foundation *Introducing the Verifiable LEI (vLEI)* [Accessed on 9 September 2021]
https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/introducing-the-verifiable-lei-vlei