

O Say Can You See... A US Digital Identity Strategy?



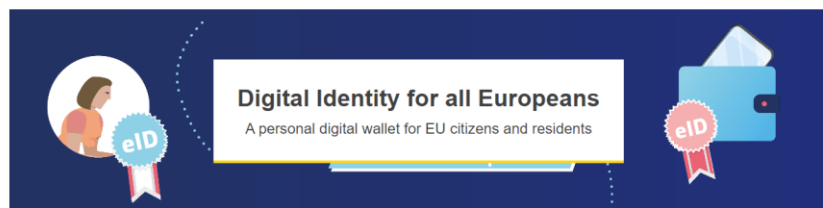
Jeremy Grant
Managing Director, Technology & Innovation
Venable LLP
@jgrantindc | jagrant@venable.com

A journey across the globe



Home > Strategy and policy > Priorities > A Europe fit for the digital age > European Digital Identity

European Digital Identity



Voilà Verified Trustmark Program is Live – ‘duty of care’ a top priority

Read More



Beehive.govt.nz

The official website of the New Zealand Government

30 MARCH 2023

Govt helps to protect New Zealanders digital identities



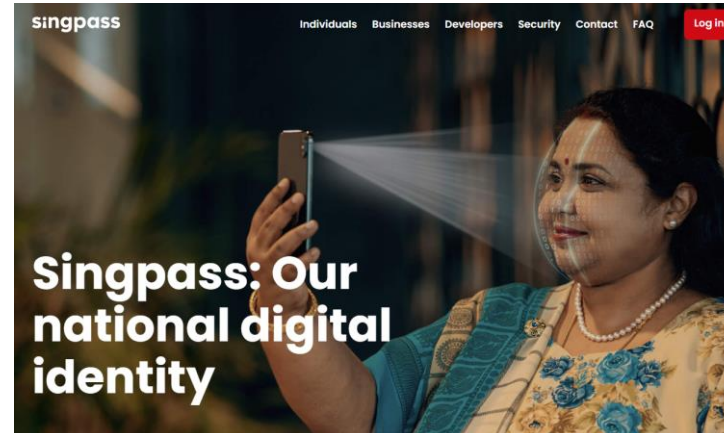
HON GINNY ANDERSEN

Digital Economy and Communications

The Digital Identity Services Trust Framework Bill, which will make it easier for New Zealanders to safely prove who they are digitally has passed its third and final reading today.

"We know New Zealanders want control over their identity information and how it's used by the companies and services they share it with. This framework will help make that easier and secure," Minister for the Digital Economy and Communications, Ginny Andersen said.

"Whether it's opening a bank account, sharing our medical history, conducting business online, or applying for Government services, it's vital we trust the systems we use, and that service providers know what's expected of them.



GOV.UK

Menu

Home > Government > Cyber security > UK digital identity and attributes trust framework alpha v1 (0.1)

Department for
Digital, Culture,
Media & Sport

Department for
Science, Innovation
& Technology

Policy paper

UK digital identity and attributes trust framework alpha v1 (0.1)

Updated 11 January 2023



#identiverse

But in the US



The last time the US had a formal digital identity strategy...2011

To be clear, there are pockets of activity...

- TSA is driving mDLs for in-person use cases (TSA checkpoints, buying booze)
- NIST and DHS are collaborating on a new project to help states with remote ID proofing use cases for mDLs
- The White House is working on an Executive Order focused on reducing identity theft in government benefits – but nothing to protect Americans from identity theft in other sectors
- The White House and GSA are focused expanding Login.gov for citizen services
- The SSA eCBSV tool will validate whether Name/DOB/SSN match their data to address synthetic ID fraud tied to new credit transactions...but not for government services
- A new Senate bill calls for the Commerce Department to create a national digital ID verification system – solely for verifying age for access to social media

...but no efforts to coordinate activities across the US government


Impacts:

- No systems to address some problems – or reliance on inefficient legacy tools
- Duplicative systems to address other problems
- No strategy to look at cross-cutting, multi-sectoral challenges
- Every time we need something to solve an identity challenge – the focus is on building a **one-off system**, rather than leverage common digital identity infrastructure

And to be clear, digital identity is critical infrastructure

DHS declared Identity as a “National Critical Function”

- April 2019: *“Provide Identity Management and Associated Trust Support Services”* decreed as one of 55 “National Critical Functions” by Department of Homeland Security
 - *“The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on either the Nation’s homeland security, economic security, public health or safety, or any combination of these.”*
- But – this has not yet translated to actions or funding that actually prioritize identity

 **CISA**
CYBER-INFRASTRUCTURE

April 2019

National Critical Functions Set			
SUPPLY	DISTRIBUTE	MANAGE	CONNECT
<ul style="list-style-type: none">• Exploration and Extraction Of Fuels• Fuel Refining and Processing Fuels• Generate Electricity• Manufacture Equipment• Produce and Provide Agricultural Products and Services• Produce and Provide Human and Animal Food Products and Services• Produce Chemicals• Provide Metals and Materials• Provide Housing• Provide Information Technology Products and Services• Provide Materiel and Operational Support to Defense• Research and Development• Supply Water	<ul style="list-style-type: none">• Distribute Electricity• Maintain Supply Chains• Transmit Electricity• Transport Cargo and Passengers by Air• Transport Cargo and Passengers by Rail• Transport Cargo and Passengers by Road• Transport Cargo and Passengers by Vessel• Transport Materials by Pipeline• Transport Passengers by Mass Transit	<ul style="list-style-type: none">• Conduct Elections• Develop and Maintain Public Works and Services• Educate and Train• Enforce Law• Maintain Access to Medical Records• Manage Hazardous Materials• Manage Wastewater• Operate Government• Perform Cyber Incident Management Capabilities• Prepare for and Manage Emergencies• Preserve Constitutional Rights• Protect Sensitive Information• Provide and Maintain Infrastructure• Provide Capital Markets and Investment Activities• Provide Consumer and Commercial Banking Services• Provide Funding and Liquidity Services• Provide Identity Management and Associated Trust Support Services• Provide Insurance Services• Provide Medical Care• Provide Payment, Clearing, and Settlement Services• Provide Public Safety• Provide Wholesale Funding• Store Fuel and Maintain Reserves• Support Community Health	<ul style="list-style-type: none">• Operate Core Network• Provide Cable Access Network Services• Provide Internet Based Content, Information, and Communication Services• Provide Internet Routing, Access and Connection Services• Provide Positioning, Navigation, and Timing Services• Provide Radio Broadcast Access Network Services• Provide Satellite Access Network Services• Provide Wireless Access Network Services• Provide Wireline Access Network Services

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

CISA.gov

Here's what this means



At a time when we have no strategy...

Identity Theft Impacts Nearly Half of U.S. Consumers, Aite Group Report Finds

Underwritten by GIACT, Aite Group Report Discovers Alarming Percentages of U.S. Consumers Impacted by Identity Theft, Application Fraud and Account Takeover



NEWS PROVIDED BY
GIACT →
Mar 09, 2021, 08:00 ET



DALLAS, March 9, 2021 /PRNewswire/ -- GIACT®, the leader in helping companies positively identify and authenticate customers, today announced a new report, *U.S. Identity Theft: The Stark Reality*, developed by Aite Group, and underwritten by GIACT, that uncovers the striking pervasiveness of identity theft perpetrated against U.S. consumers and tracks shifts in banking behaviors adopted as a result of the pandemic.

[Click here to download the report](#)

According to the report, from 2019 to 2020, almost half (47%) of U.S. consumers surveyed experienced identity theft; well over one-third (37%) experienced application fraud (i.e., the unauthorized use of one's identity to apply for an account), and over one-third (38%) of consumers experienced account takeover over (i.e., unauthorized access to a consumer's existing account) over the past two years.



Identity-related cybercrime has soared to record levels – impacting millions of Americans

Impacting not just government programs – but banking, health, retail, and other sectors

“Analysis of the over 3 million Suspicious Activity Reports that financial institutions filed with us in 2021 shows that the majority include reference to potential breakdowns in the identity verification process—verification, impersonation, and compromise.”

-Jimmy Kirby, Deputy Director, Financial Crimes Enforcement Network (FinCEN)



<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-deputy-director-jimmy-kirby-during-2022-federal>

At a time when we have no strategy...

The IRS is backing down from asking for selfies to verify identities



Susan Tompor

Detroit Free Press

Published 4:35 p.m. ET Feb. 7, 2022 | Updated 4:56 p.m. ET Feb. 7, 2022

[View Comments](#)



After a great deal of pushback, the Internal Revenue Service on Monday finally concluded that basically, it's OK, the IRS doesn't need to see your selfie to verify that you are you.

Monday, the IRS announced plans to drop a controversial step to use facial recognition to verify IDs online.

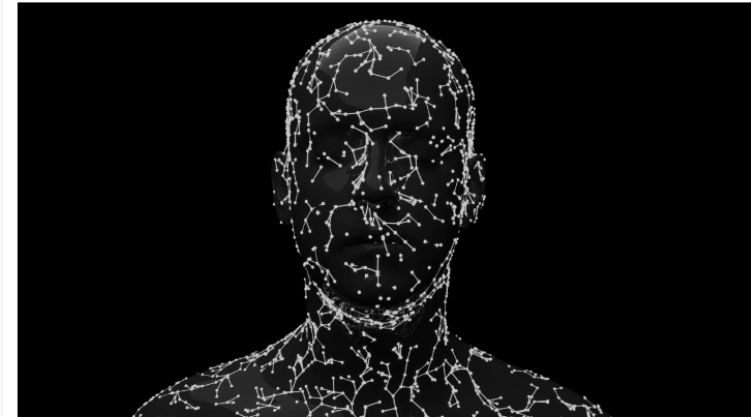
The IRS said that it will move away from using a third-party service that used facial recognition to help authenticate people who needed to create new online IRS accounts to gain access to such things as the IRS Child Tax Credit Update Portal and obtain a tax transcript online.

Not surprisingly, taxpayers and those concerned about privacy never embraced the idea of sending a picture to to the IRS to open an online IRS account. And many expressed concerns that the technology may be less reliable for people of color or older people.

MITRE: White House biometrics definition requires rethink

OSTP conflated three distinct concepts as biometrics, which will lead to confusion as it attempts craft an AI Bill of Rights.

BY DAVE NYCZEPIR • FEBRUARY 9, 2022



(Getty Images)

MITRE's Center for Data-Driven Policy recommended the White House redefine biometrics as it develops an Artificial Intelligence Bill of Rights, in a request for information response submitted last month.

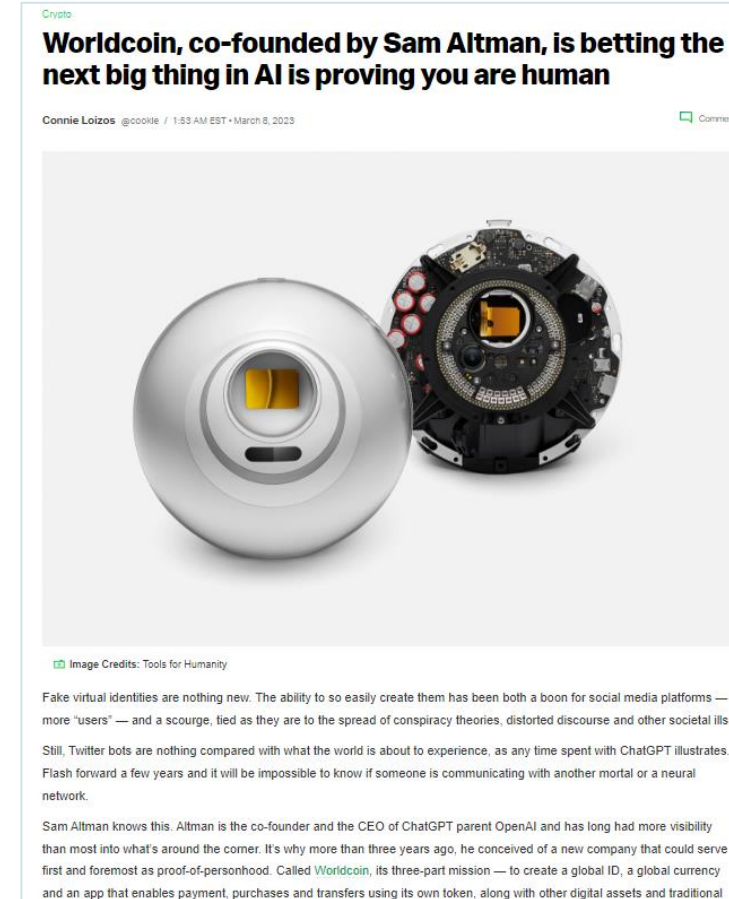
Within its RFI, the [Office of Science and Technology Policy](#) married [biometrics](#) for identification with technology for inferring emotion or intent and medicine's understanding of the term as any biological-based data. [MITRE](#) would rather OSTP

SHARE



Privacy and equity concerns around identity have grown more complex

At a time when we have no strategy...



The rise of AI has people worrying how we'll know who is human

Is identity the new “salmon?”



“The Interior Department is in charge of salmon while they’re in freshwater, but the Commerce Department handles them when they’re in saltwater.”

“And I hear it gets even more complicated once they’re smoked.”

-Barack Obama, 2011

ID Theft Executive Order?



- **Executive Order on Preventing Identity Theft in Public Benefits Programs:** In the coming weeks, the President will announce a new Executive Order with broad government-wide directives, building on steps taken in 2021, to prevent and detect identity theft involving public benefits, while protecting privacy and civil liberties and preventing bias that results in disparate outcomes. The EO will also direct new actions to support the victims of identity fraud.
- Announced March 1, 2022
- Still not released as of May 2023

White House mulls scaling up Login-dot-gov to reach every American



DILOK KLAISATAPORN/GETTY IMAGES



By Natalie Alms,
Staff Writer

FEBRUARY 21, 2023

A draft of a long-awaited executive order covering digital identity includes a push to make government-owned Login-dot-gov an option for most federal benefits programs.



The White House appears set to give Login-dot-gov, a digital identity service run by the General Services Administration, a leading role in providing access to public benefits programs, according to a draft executive order obtained by FCW.

No concerns there...

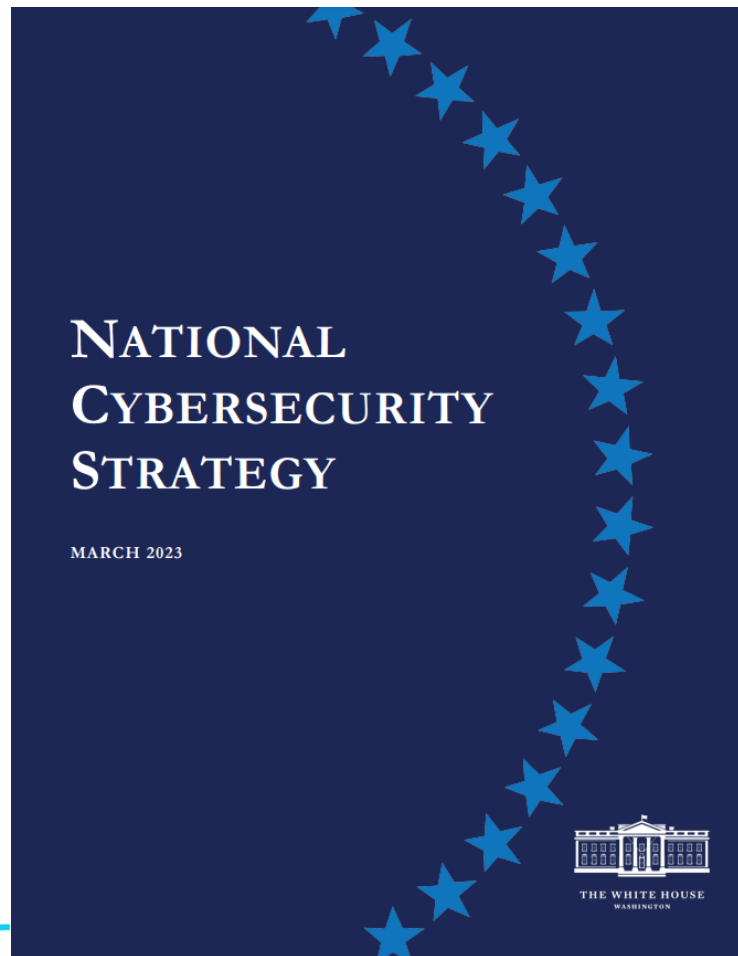


Office of Inspections
Office of Inspector General
U.S. General Services Administration

GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards

JE23-003 (Redacted)
March 7, 2023

A glimmer of hope



STRATEGIC OBJECTIVE 4.5: SUPPORT DEVELOPMENT OF A DIGITAL IDENTITY ECOSYSTEM

Enhanced digital identity solutions and infrastructure can enable a more innovative, equitable, safe and efficient digital economy. These solutions can support easier and more secure access to government benefits and services, trusted communication and social networks, and new possibilities for digital contracts and payment systems.

Today, the lack of secure, privacy-preserving, consent-based digital identity solutions allows fraud to flourish, perpetuates exclusion and inequity, and adds inefficiency to our financial activities and daily life. Identity theft is on the rise, with data breaches impacting nearly 300 million victims in 2021 and malicious actors fraudulently obtaining billions of dollars in COVID-19 pandemic relief funds intended for small businesses and individuals in need. This malicious activity affects us all, creating significant losses for businesses and producing harmful impacts on public benefit programs and those Americans who use them. Operating independently, neither the private nor public sectors have been able to solve this problem.

The Federal Government will encourage and enable investments in strong, verifiable digital identity solutions that promote security, accessibility and interoperability, financial and social inclusion, consumer privacy, and economic growth. Building on the NIST-led digital identity research program authorized in the CHIPS and Science Act, these efforts will include strengthening the security of digital credentials; providing attribute and credential validation services; conducting foundational research; updating standards, guidelines, and governance processes to support consistent use and interoperability; and develop digital identity platforms that promote transparency and measurement. Acknowledging that States are piloting mobile drivers' licenses, we note and encourage a focus on privacy, security, civil liberties, equity, accessibility, and interoperability.

In developing these capabilities, our digital identity policies and technologies will protect and enhance individual privacy, civil rights, and civil liberties; guard against unintended consequences, bias, and potential abuse; enable vendor choice and voluntary use by individuals; increase security and interoperability; promote inclusivity and accessibility; and improve transparency and accountability in the use of technology and individuals' data.

Although...

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023



Program authorized in the CHIPS and Science Act, these efforts will include strengthening the security of digital credentials; providing attribute and credential validation services; conducting foundational research; updating standards, guidelines, and governance processes to support consistent use and interoperability; and develop digital identity platforms that promote transparency and measurement. Acknowledging that States are piloting mobile drivers' licenses, we note and encourage a focus on privacy, security, civil liberties, equity, accessibility, and interoperability.

Up next: the Implementation Plan

- The National Cybersecurity Strategy lays out the strategic objectives; the Implementation Plan is where we'll learn more about action.

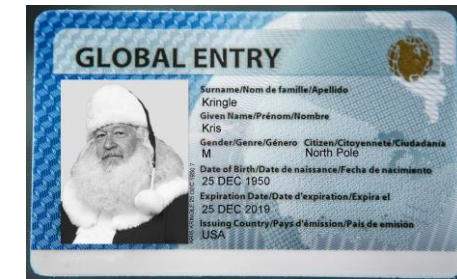
What should they do?

- A “distinctly American approach”
- No new national ID
- No new identity systems
- Instead...focus on the “Identity Gap”



Focus on the Identity Gap

- The “identity gap” – the U.S. has many nationally recognized, authoritative identity systems
- All are trapped in the paper world



In Simple Terms...

If I've gone through the process of having an agency vet my identity once – can I ask that agency to vouch for me when I need to prove who I am to another party?

America's legacy paper-based systems should be modernized around a privacy-protecting, consumer-centric model that allows consumers to ask the government agency that issued a credential to stand behind it in the online world – by validating the information from the credential.



How could we get there?


1. The White House could decide to launch digital identity initiative – following through on the National Cybersecurity Strategy
2. Congress could pass a law to establish an initiative



The Improving Digital Identity Act

- Bipartisan digital ID legislation introduced to coordinate a government-wide approach to identity validation services
- Senate sponsors: Kyrsten Sinema (I-AZ), Cynthia Lummis (R-WY)
 - Approved by Senate Homeland Security and Government Affairs Committee March 29th!
- House sponsors: Bill Foster (D-IL), John Katko (R-NY)*, Jim Langevin (D-RI)*, Barry Loudermilk (R-GA)



The background of the slide features three classical stone pillars, likely from the Lincoln Memorial, set against a clear blue sky. The pillars are arranged in a row, with the one on the right being the most prominent and tallest. The text is overlaid on the upper portion of the image.

A “whole of
government”
approach – covering
Federal, State & Local

NIST Framework of
standards, policies, and
rules – that any agency
can use to create
interoperable services
that set a high bar for
security and privacy *

Grant dollars to states to
modernize legacy ID
systems to support
digital ID

Three Pillars to Better Identity

*Included in CHIPS & Science Act of 2022

THANK YOU!



Jeremy Grant
Managing Director, Venable LLP
@jgrantindc | jagrant@venable.com