netStudio

An Indra company

Digital Identity

Necessità, adozione, evoluzione

24/05/2024

Giacomo Parravicini

gparravicini@netstudio-sia.com

All the information contained in this document and its annexes is confidential, and may only be used for the purpose of being evaluated by the recipient (whether client, supplier, collaborator, partner, etc.) of the same and for the sole purpose of conducting the business dealings, or otherwise, that motivate the sending of the document (hereinafter, the "Purpose").

The information presented herein is prepared by NET STUDIO (a joint-stock company with a single shareholder), subject to the management and coordination of SISTEMAS INFORMATICOS ABIERTOS, S.A.U., a company belonging to the Indra Group, with C.I.F. A82733262 and registered office at Av. de Bruselas, 35, 28108 Alcobendas (Madrid), Spain and cancels and replaces the previous ones, and is a trade secret (also referred to in certain jurisdictions as a trade secret), and may also be protected by copyright, related rights, patent, utility model and/or industrial design and therefore its disclosure and/or transmission to third parties is strictly prohibited without the prior, express and written permission of SIA.

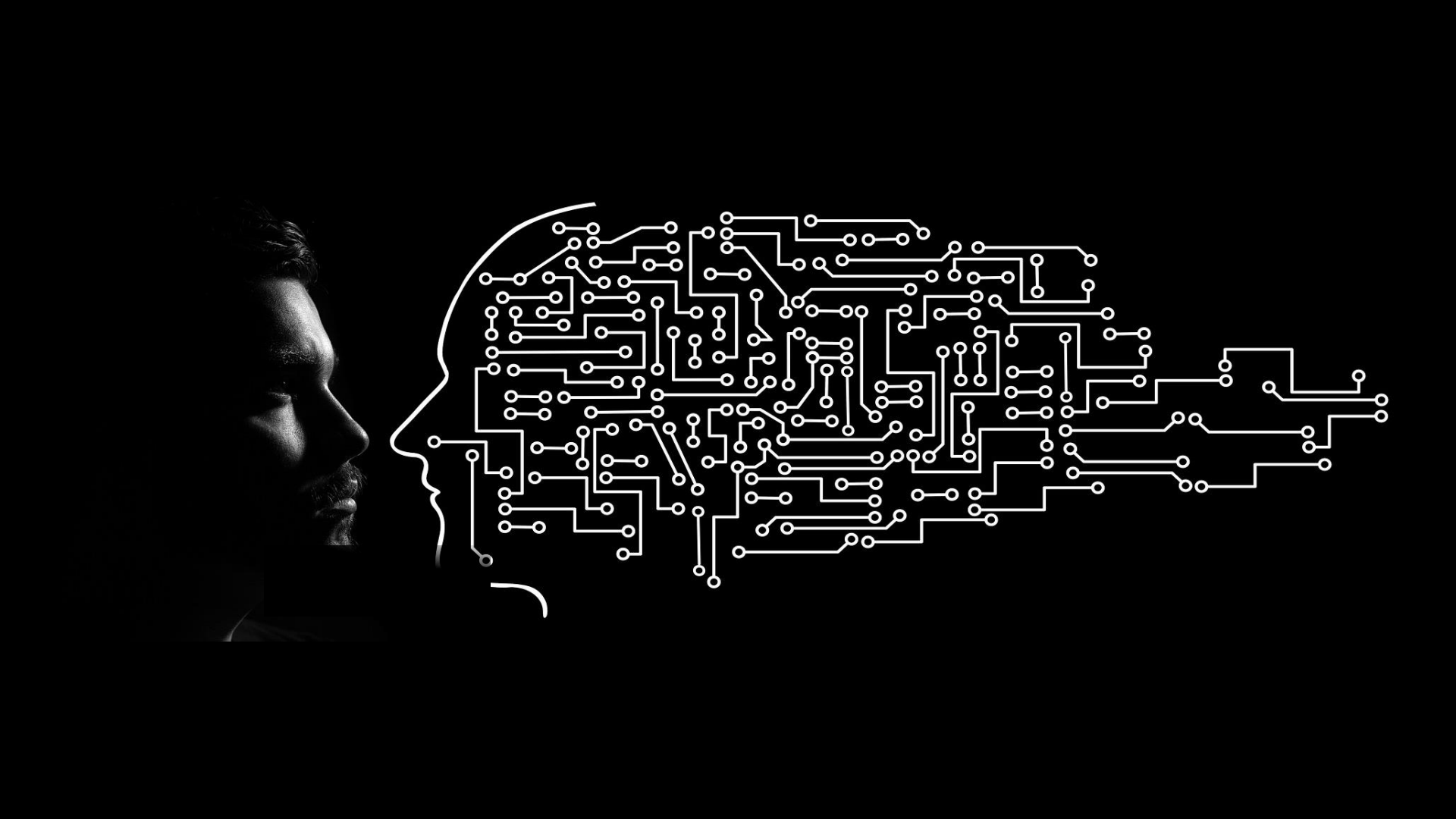
Access to the confidential information by the personnel of the recipient thereof, or by the personnel of those third parties authorized by SIA to access the confidential information, shall be limited as much as possible, being limited only to those persons whose access is strictly necessary, and the recipient of the confidential information must guarantee that it informs such persons of the confidential and proprietary nature of the information as well as of the Purpose, ensuring that such personnel treat the confidential information solely and exclusively for the Purpose, and refraining from any disclosure.

Upon completion or termination of the Purpose, the customer must return to SIA all confidential information without retaining any copies thereof and may not use in any manner or for any purpose the confidential and/or proprietary information provided by SIA unless previously and expressly authorized to do so in writing by SIA.

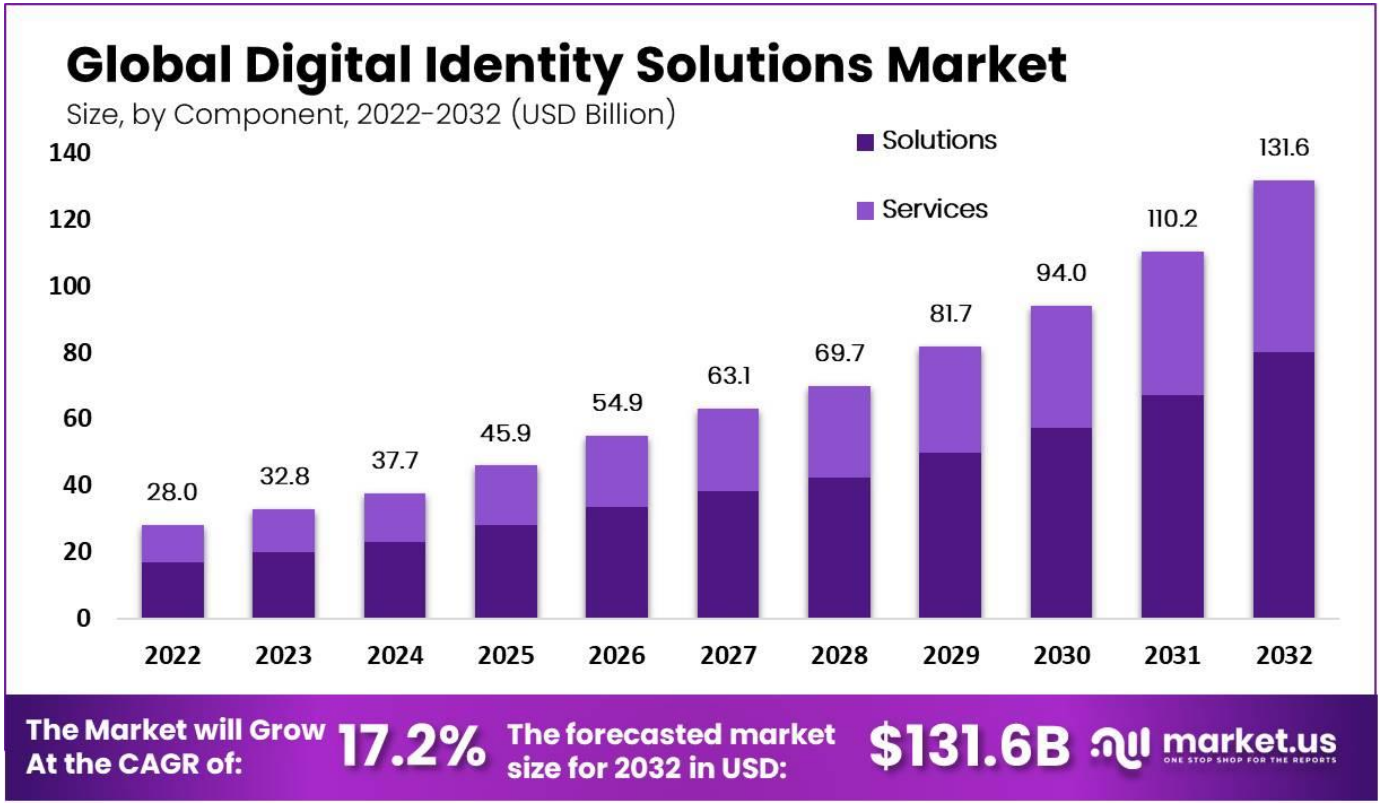
The recipient of the Confidential Information, after completion of the Purpose, may not use in any manner or for any purpose the Confidential and/or Proprietary Information provided by SIA.

Indice

1. The Identity Context
2. Getting a Digital Identity
3. Using a Digital Identity
4. Trends and future of Identity
5. Q&A



Identity Market



Parliamo di identità digitale

Cosa intendete per identità digitale ed in cosa si differenzia dall'identità fisica ?

Fisica:
- Caratteristiche tangibili (Volto, CI, Passaporto)
- Gestita da enti governativi

Digitale:
- Informazioni online, email, profili social.
- Controllata da piattaforme private

- Entrambe necessitano di misure di sicurezza per prevenire frodi ed usi non autorizzati

Parliamo di identità digitale

Quali sono gli elementi chiave che compongono un'identità digitale ?

- Dati Personali
- Credenziali di accesso
- Attributi biometrici
- Certificati Digitali
- Attività Online

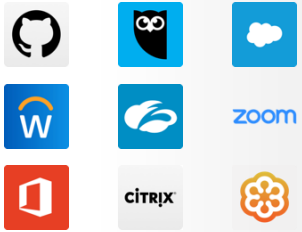
Parliamo di identità digitale

Quali sono i principali rischi e le sfide legate alla gestione dell'identità digitale ?

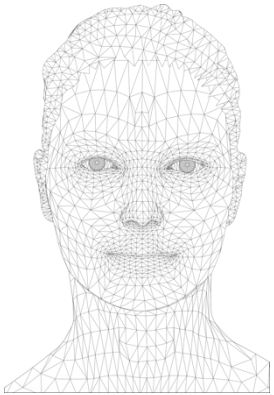
- Furto d’identità
- Violazione dei dati
- Gestione delle password
- Vulnerabilità dei sistemi
- Usabilità vs Sicurezza

Why do we need digital identities?

For
Customer
interaction



For work



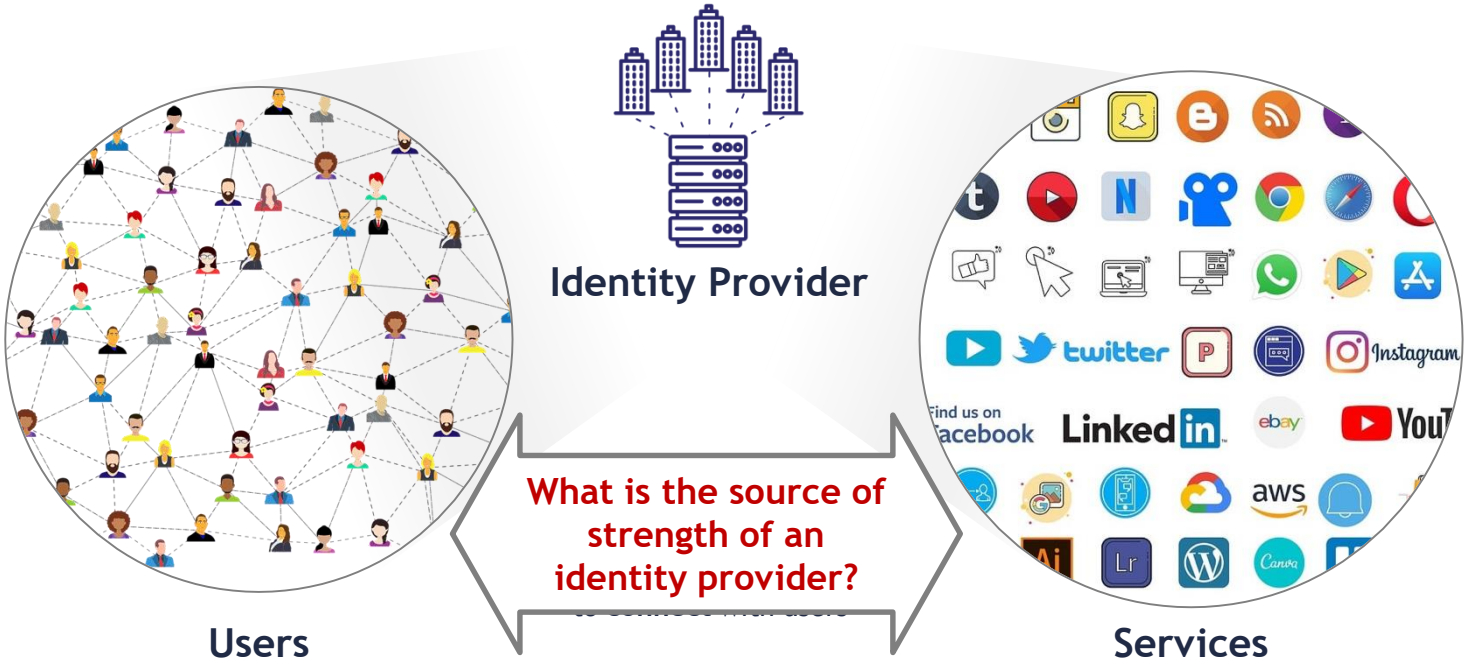
For social
interactions

For Citizen
interaction

netStudio

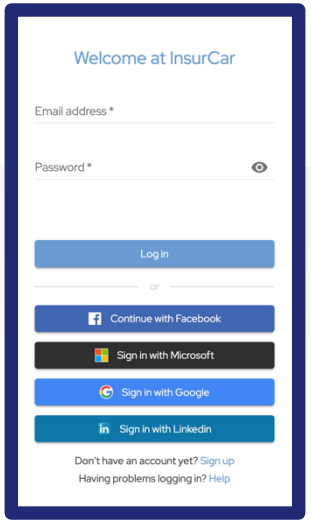
An Indra company

The need for identity providers



Some identity providers that you already know

Users



Identity Provider

Insurance Company
(Service Provider)

Some identity providers that you don’t notice

Your gateway to travel services

Your gateway to citizen services

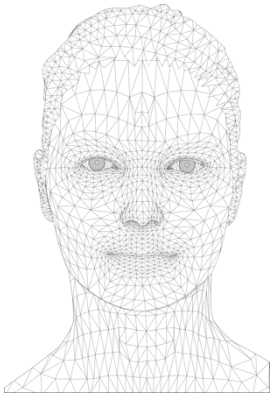
Your gateway financial services

Your gateway to commerce

Your gateway to healthcare

Your gateway to communication services

Digital identity and privacy are interrelated concepts



- Name
- Address
- Phone number
- Email Address
- Date of Birth
- National ID Number
- Tax Identification
- Shoe size
- Waist size, height

Can users **trust** any **service provider** with any data?

Can users **trust** any **identity provider** with any data?

Can user identity data (**attributes**) be stored anywhere?


Grow Your Customer Value Through Trust
Protected
Authorizations
Trusted
Strong Authentication
Known
Digital Onboarding
Recognized
User Profile, Consent
Anonymous

2024 Trust Index Ranking

#2024TrustIndex

https://cpl.thalesgroup.com/digital-trust-index

The research was carried out among 12,426 general respondents in Australia, Brazil, Canada, France, Germany, Japan, Singapore, South Africa, The Netherlands (NL), the United Arab Emirates (UAE), the United Kingdom (UK), and the United States of America (USA).

netStudio

An Indra company

2024 Trust Index Ranking

#2024TrustIndex

Customer were asked what sector they were most comfortable to share their personal information with

You blink, you lose- customers are time conscious

#2024TrustIndex

Consumers want their interactions to be quick convenient and hassle free.

22%

Over a fifth **give up within a minute they're having a frustrating online experience** – with the likes of complicated onboarding processes, password resets and having to re-enter personal information

No compromise on MFA – consumers want better experiences and Security!

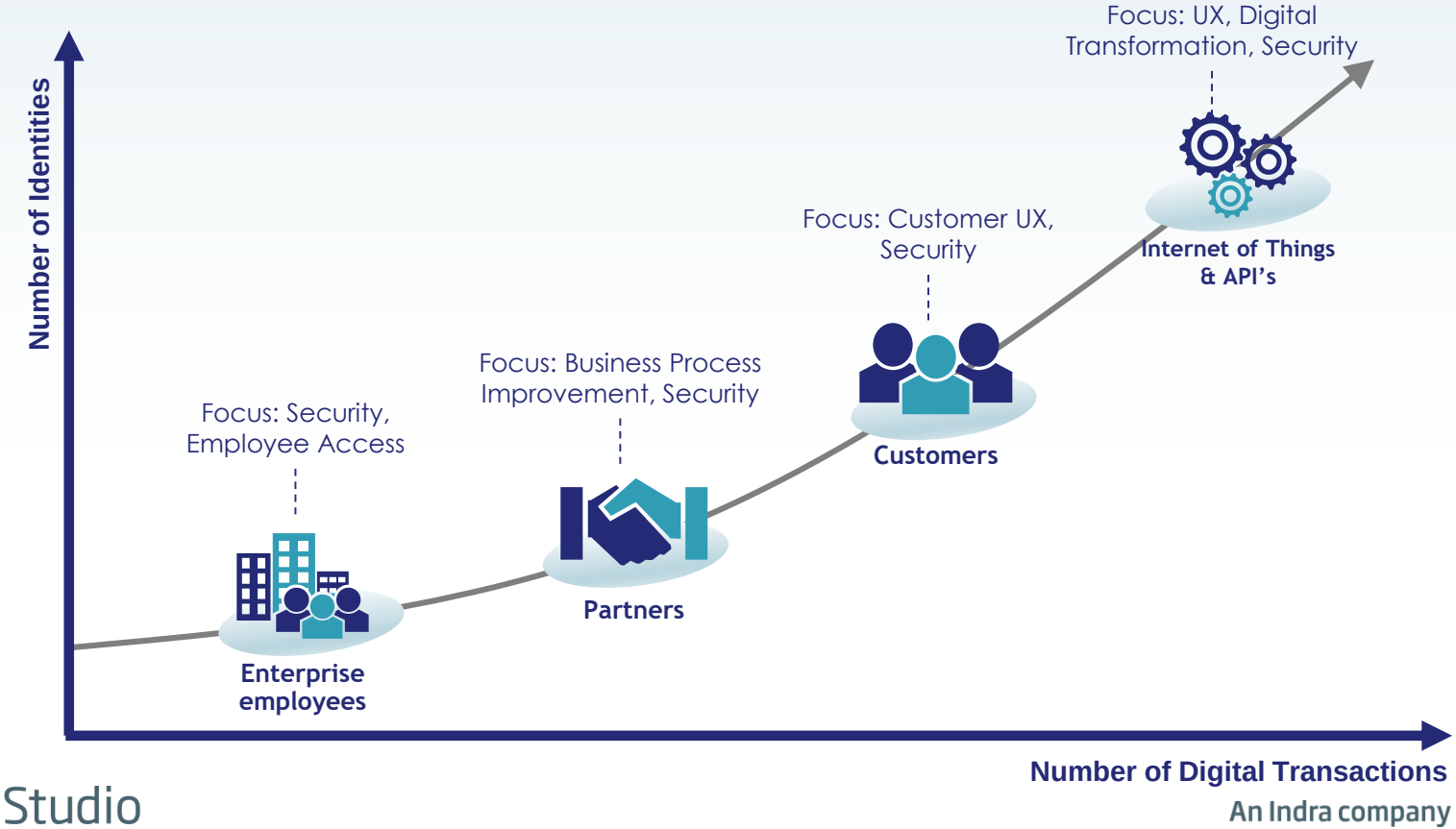
#2024TrustIndex

Not just regulations or mandates, your customers expect you to offer Multi-factor authentication

81%

User Types and expectations

Evolution of Digital Identities



netStudio

An Indra company

How businesses are transforming to address these expectations

External Transformation

Introducing **new channels** to interact with customers

Building new business models by **digitalizing** offers

Using analytics to build more user-friendly **customer experiences**

Internal Transformation

Improving employee productivity with modern **Productivity Apps**

Reducing cost of operations by leveraging **Cloud Computing** and **IoT**

Introducing modern ways of working like **remote** or **hybrid work** to improve talent retention

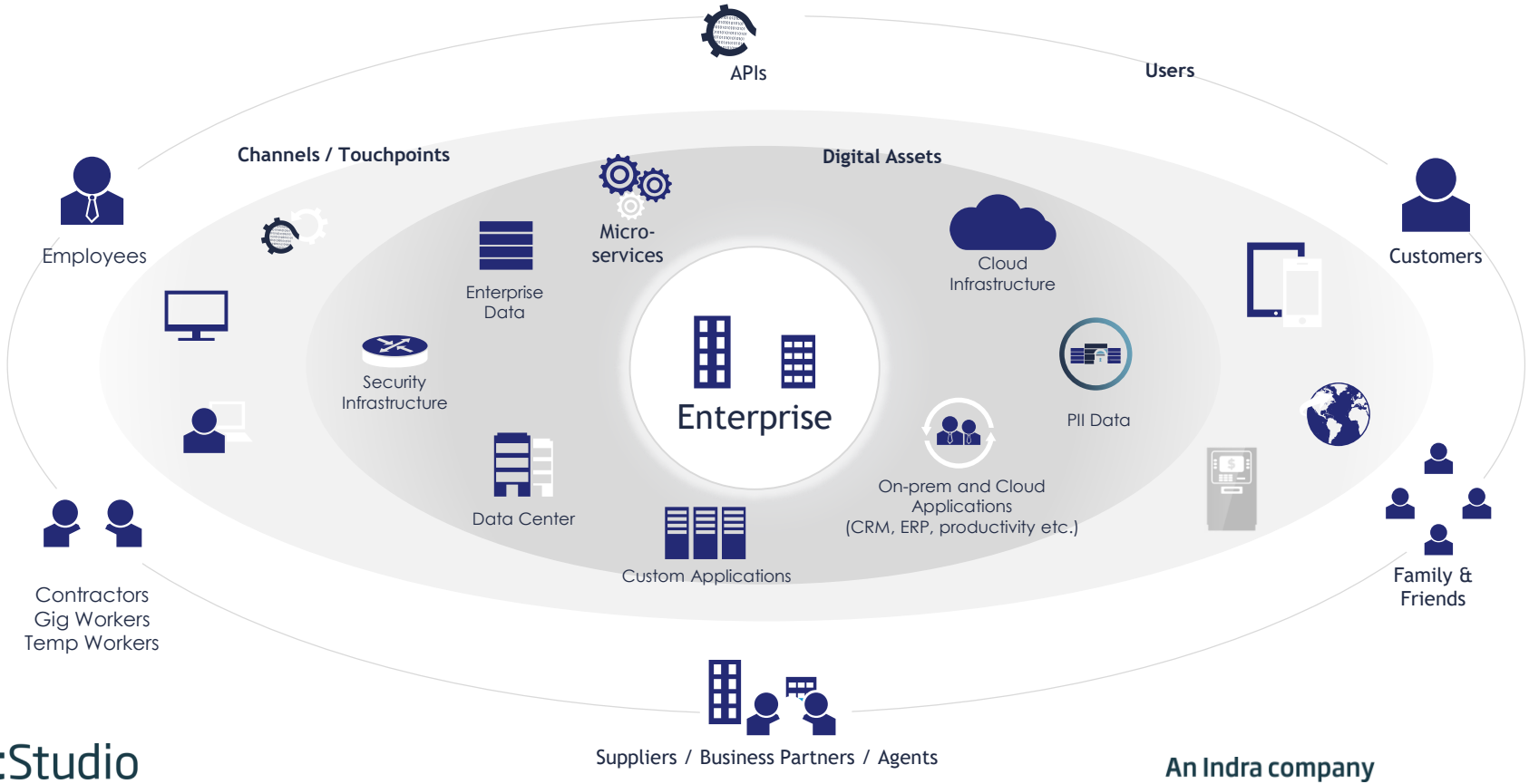
What we're hearing from organizations

Help me... Get to market faster, support our digital transformation with security by design

Help me... To support consumers with a seamless and frictionless customer journey

Help me... Create a program for repeatable operations towards my partners and suppliers

Enabling access to digital assets for multiple users is an imperative



netStudio

An Indra company

Identity & Access is core to the digital user journey

EXPLORE | CONSIDER | PURCHASE | USE | ABANDON

Registration

Enable users to prove their identity

Let users sign up and log in with their social ID

Provide consent to terms of service and data collection

Authenticate

Manage preferences

Authorize

Access Applications

Delegate Access to others

Delete account

LEAVE

USE

LOG IN

SIGN UP

netStudio

An Indra company

Identity Capabilities for the entire digital journey

Identity Verification

- BYOI
- Document Verification, Liveness Detection

Authentication

- Digital ID Wallets, Mobile ID, Digital Driver's License
- Strong Auth, Phishing-resistant Authentication, Passwordless
- Single Sign-on

Authorization

- Adaptive Access
- Fine-grained Authorization
- Delegation and Relationship Management

Deletion

- Account Deletion
- Right to forget

SIGN UP → LOG IN → USE → LEAVE

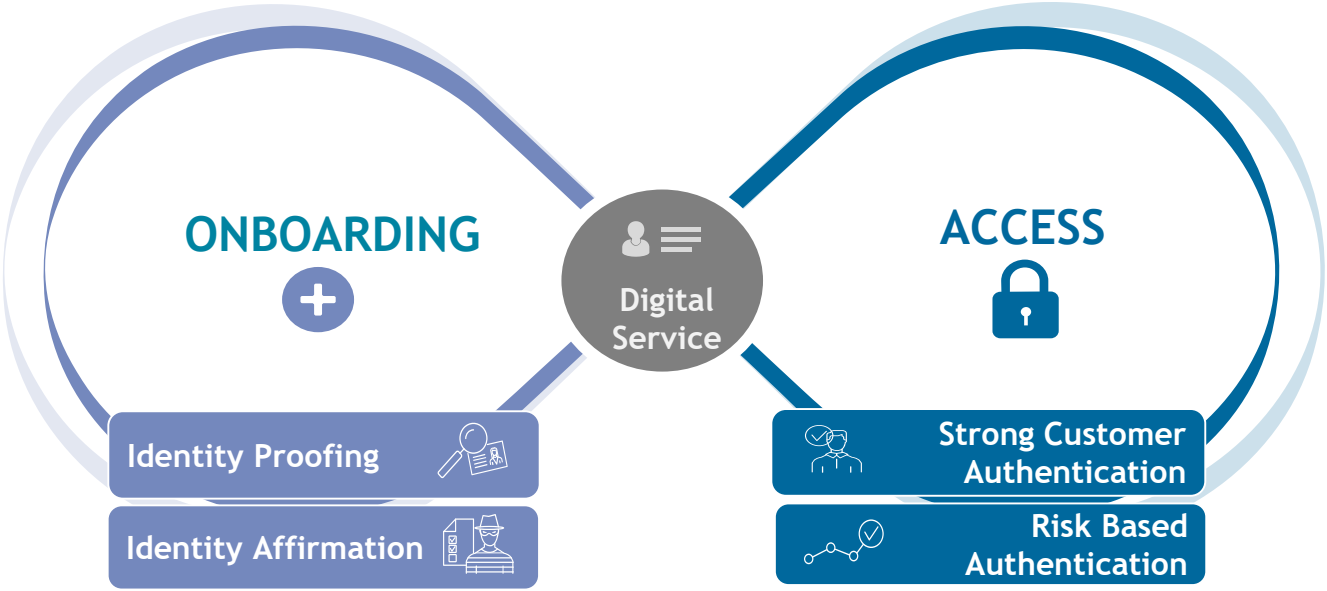
- User Journey Orchestration, Authentication Journey
- Consent and Preference Management
- Progressive Profiling
- Risk Management

netStudio

An Indra company

Getting a Digital Identity

The journey loop



ORCHESTRATION

FRICTIONLESS USER EXPERIENCE

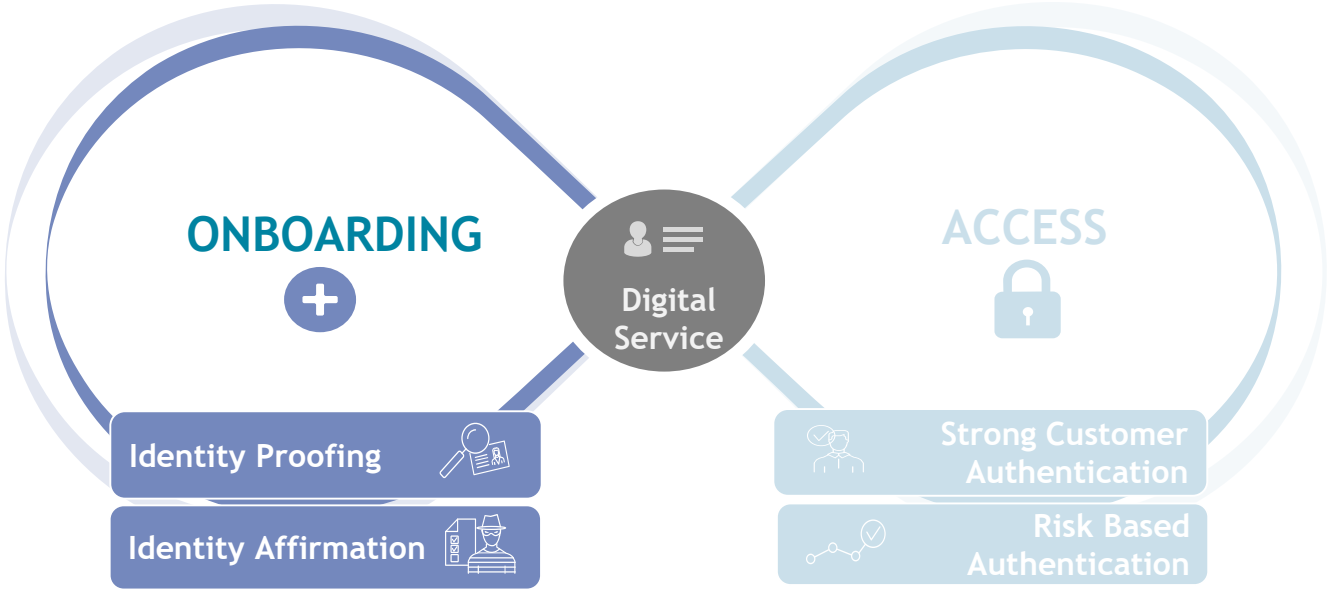
ENHANCED SECURITY

REGULATORY COMPLIANCE

netStudio

An Indra company

The journey loop



ORCHESTRATION

FRICTIONLESS USER EXPERIENCE

ENHANCED SECURITY

REGULATORY COMPLIANCE

Onboarding pain points

- Minimize application fraud and prevent mule account creation
- Secure and fast track onboarding process
- Minimize abandonment rate
- Comply with regulations (eg: PCS2)
- Improve risk assessment over time while keeping fraud level at its minimum
- Manage business rules and actions over time while security concerns are moving ahead

Securing customer onboarding

A full digital onboarding process need multiple verification layers.

ID document possession and biometric association:

- Document authentication
- Face verification
- Liveness detection

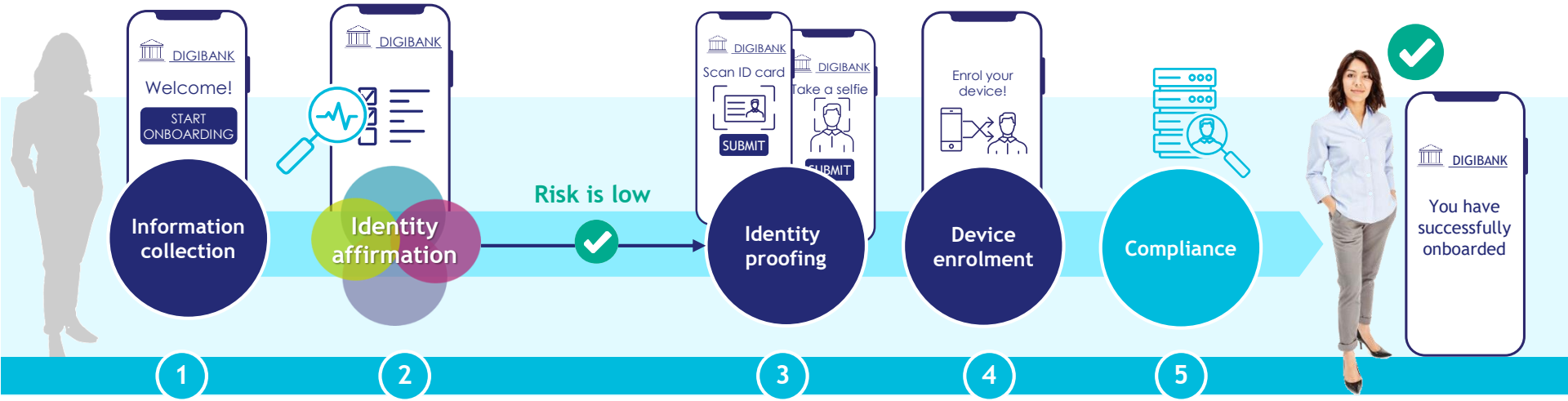
Supporting evidence for the identity claim with additional background checks:

- User attributes
- Device details
- Network information

Identity compliance process:

- Banking Anti Money Laundry (AML) watch & sanction lists
- Address verification

The digital onboarding journey



User entered information:
- mobile phone
- email...

Background checks:
- Device intelligence
- Behavioral analytics
- Behavioral biometric
- Consortium intelligence

- Document authentication
- Facial recognition
- Liveness detection

- User authentication
- Email verification
- Approve OOB

- Backend checks
- AML watch lists / sanction lists

BENEFITS

- ✓ Increased confidence that identity proofing is safe
- ✓ Avoid unnecessary identify proofing costs when risk is high

netStudio

An Indra company

Onboarding Approaches

1

☑ Document Authentication

2

☑ Face Match service

☑ Passive Liveness Detection

3

☑ Electronic ID verification NFC reading

Key element to consider for an accurate verification

1

Standard Image Capture & computer vision machine learning

Doc Authentication

Validate if the document was issues by a governing authority

+40 ✓checks per doc

&

Tampering Detection

Alert a client about a potentially tampered document

photo, text, copy, screen

Passed

Attention

Failed

netStudio

An Indra company

Identity Proofing Conversion Rate expectations

1

85%

A successful onboarding ratio is about 85%+ conversion rate

<3%

You want to contain ID fraud to its minimum ratio

False Acceptance Rate

FAR

<4%

You want to reduce wrong rejection of true customers

False Response Rate

FRR

netStudio

An Indra company

About Document Verification

- Microprint text & security threads
- Validation of special paper & ink
- MRZ vs visual inspection zone
- Barcode reading
- OCR text
- State seals & holograms
- Pattern detection
- Photo & text substitution (ML)
- Original document (ML)
- Screen detection (ML)

About Performances

- Average performance highly depend on image quality
- Image resolution, blurriness, cropping are essential
- SDK /webSDK to ensure image quality requirements
- We recommend NFC whenever available

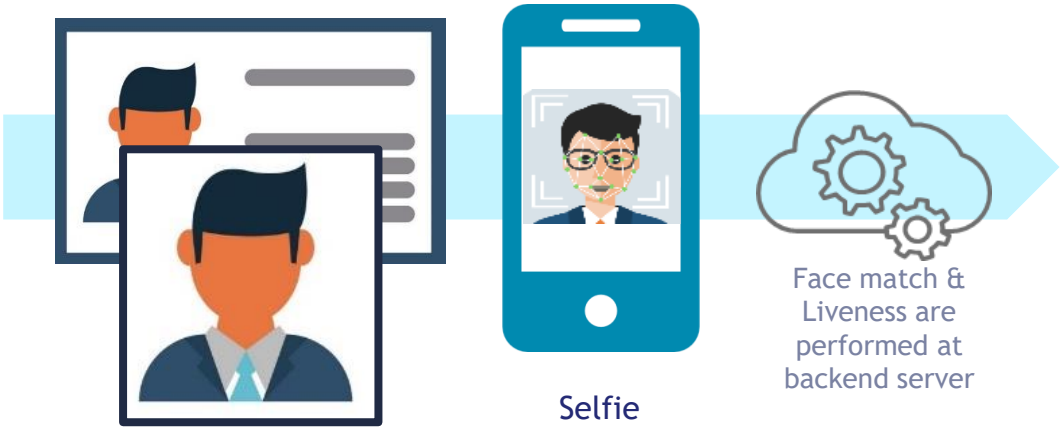
netStudio

	Pass Rate
UK	80%
Romania	75%
Panama	98%
Canada	88%
Colombia	75%
Jordan	88%
Armenia	87%

Using Facial biometric verification

2

Biometric face match is the easiest way for binding a physical individual to the processs



- Mobile & web
- **Passive Liveness detection**
- Frictionless user experience
- Mitigate photo/video substitution
- Certification for presentation attack detection (PAD level 2) highest
- Face algo rank #8 with NIST US

netStudio

An Indra company

About Facial & Liveness Performance

Passive Liveness for **frictionless user experience**

Mitigate **photo/video** fraud attempt

Presentation Attack Detection Certification (PAD level 2)

FAR less than 2%

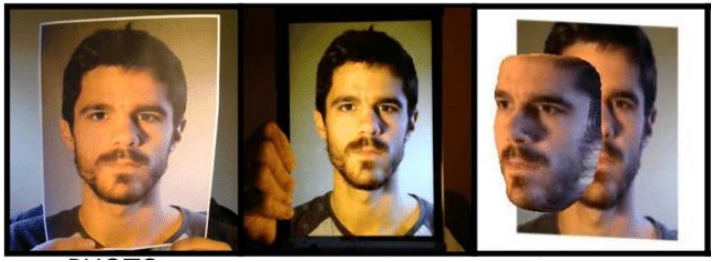
netStudio

An Indra company

AI - Threat or Opportunity?

2

- ID impersonation
- 3D masking
- Image or Video Presentation attacks
- Video Injections
- Deepfakes



ML is providing new typology of attacks but also counter measures capabilities: video injection and presentation attack detection

Electronic ID documents

98%

2%

Tap & Read user experience

Government Certificate Scheme : **nonrepudiation** and **anti cloning**

Strongest Cryptographic electronic ID Authentication

Cryptographic Assessment of the Chip Contents

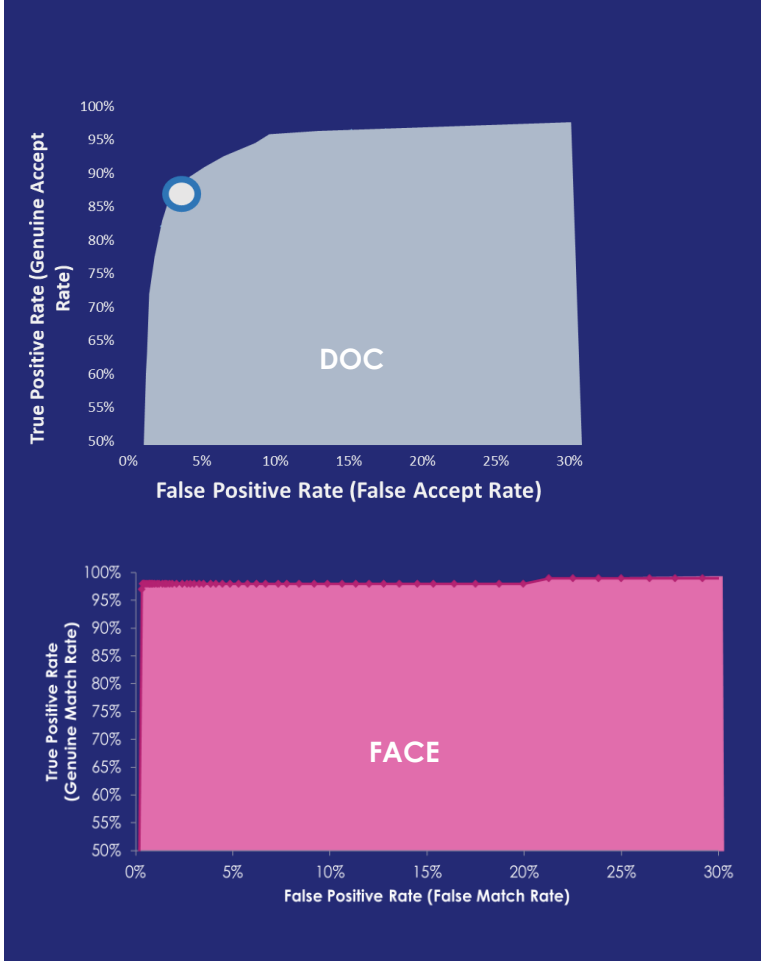
Validates Document Signer Certificate and Country of Origin (incl. Revocation Checking)

Average performance rate

> **Document verification**
88% true positive rate vs 4% false positive rate

> **Face technology**
98% True Positive Rate vs 2,11% False Positive Rate

> **Face + Passive Liveness technology**
False Positive Rate <1.2%



netStudio

An Indra company

Evolution of “Identity” & Impacts on on-boarding

Today

Computer Vision ML
Biometric | Liveness
Manual Review
Video call
Agent /attended

Near Future

Electronic ID
NFC eKYC

Tomorrow

ID Wallet
Mobile ID | DL
Attributes & Consent

The challenge

REACH
USABILITY
SECURITY
CONVERSION
COST

netStudio

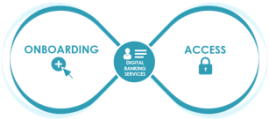
An Indra company

Identity affirmation

netStudio

An Indra company

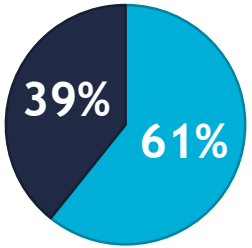
Case study - Identity affirmation stops application fraud



IDV + Identity Affirmation

Identity Affirmation is vital to onboarding service:

- Marketing campaigns attract fraudsters who try to benefit from reward programs
- Regular waves of attacks with fraudsters constantly modifying their modus operandi
- Fraud Expert uncover fraud pattern and implement counter-measures



9 waves of attacks in **18** months

BREACHED DEVICES

DISPOSABLE EMAILS

VELOCITY ATTACKS

IP MASKING

SPOOFED NETWORK

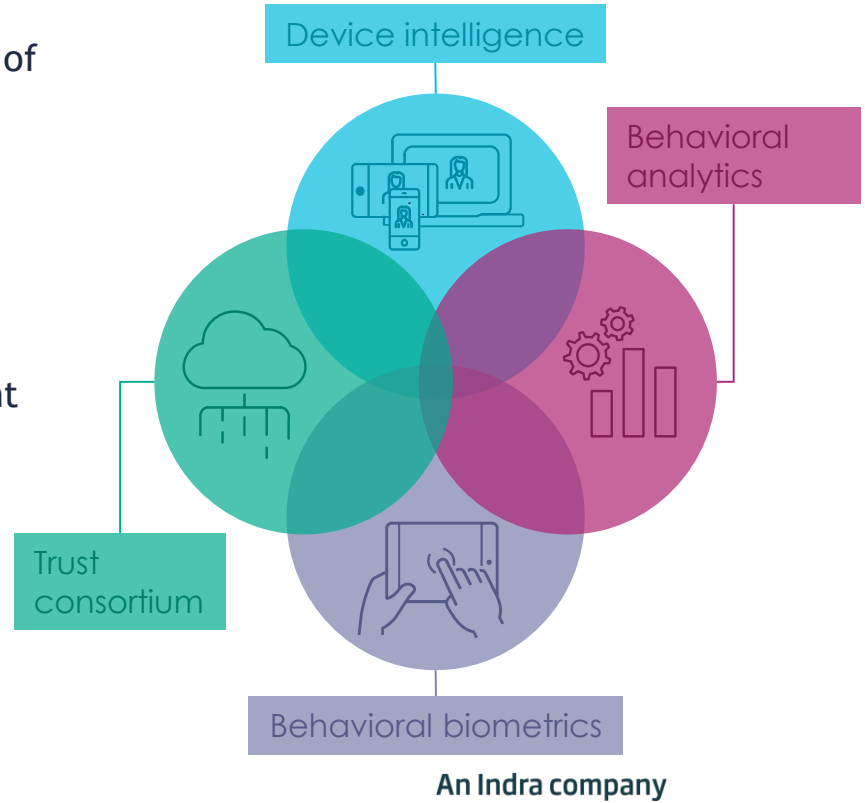
netStudio

An Indra company

Identity affirmation to increase level of confidence

Identity affirmation technology harnesses the power of four layers of intelligence. Each layer analyzes anomalous activities from different perspectives to identify high risk before any damage occurs.

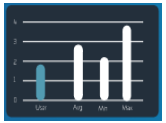
Together, they create a dynamic profile of each event that protects future customers and businesses.



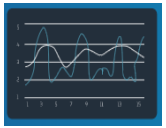
netStudio

An Indra company

Identity affirmation in action: New Account fraud



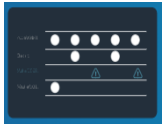
Too little time spent on page: the average user takes 3 minutes to fill out this form. This user spent 125 seconds on the page, well under the average.



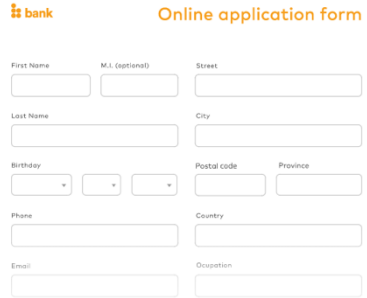
Suspicious typing: The long pauses and constant corrections – especially filling out name and last name – show the user is not familiar with the information.

Suspicious window changes: The applicant used keyboard shortcuts to switch between windows. Human farms often do this to check an adjacent Excel sheet with stolen identity information.

Mouse distance was too short: The total distance travelled by the mouse shows how well a user knows the form. This mouse travelled 5000 pixels, when the average is 13,000 pixels.



Suspicious device: The device used to fill out the form shows a type of browser version that doesn't exist.



Device intelligence

Why it matters?

- **90%** of trusted interactions come from a known device
- **97%** of fraud comes from an anomalous device or network

Device intelligence allows to

- Accurately recognize returning devices
  - Better recognize legitimate users
  - Elevate level of risk when a new device is used
- Detect anomalies in network and device which can betray fraudsters activities

Behavioral biometrics

Behavioral biometrics looks at inherent user behavior to prevent Account Takeover.

This layer analyses how a user types, moves the mouse, or holds the device, among others.

Key metrics

- Keystroke count
- Aggregate time in field
- Total time spent entering data
- Click count
- Characters per second
- Words per minute
- Number of touch events
- Time from page load to first keystroke
- Time from final keystroke to page submit
- Average orientation
- Field activation method
- Mouse travel distance
- ....

Different types of profile

Individual profile

Population profile

BOT detection

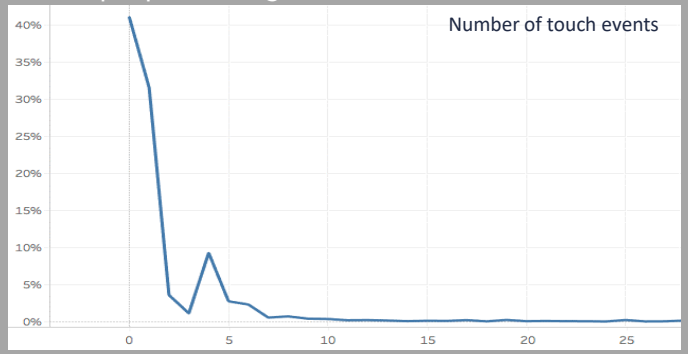
netStudio

An Indra company

Behavioral biometrics - Population profile

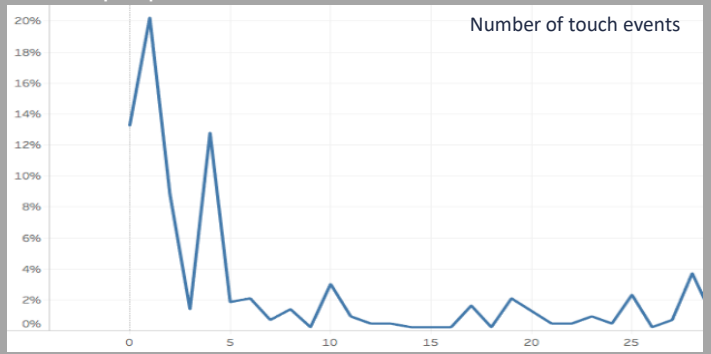
For a group of users, aggregate individual interactions to create an overall ‘good user’ and ‘fraudulent user’ profile

Sample profile of good users



> Legitimate users tend to have fewer than 8 touch events

Sample profile of fraudulent users



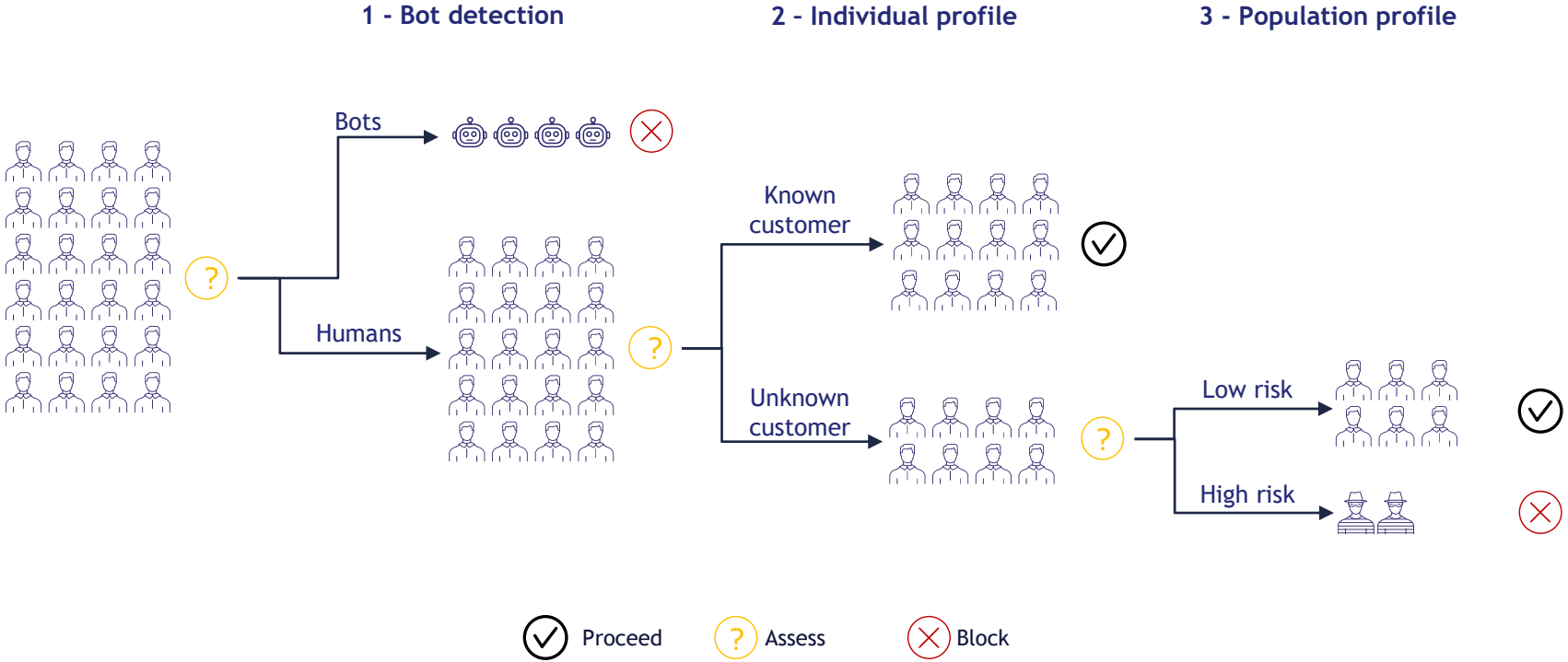
> Users associated with confirmed fraud have tendencies to have 10+ touch events

Same analyses are repeated for all events:
Keystroke count, time in field, words per minute…

netStudio

An Indra company

Combine technologies to minimize friction for good users



netStudio

An Indra company

Trust consortium

Aggregates selected data points across the client base to build reputation analysis.

It builds fraud and reputation scores based on previous scores where the data points were seen.

What's in the consortium

- IP address
- Device
- Account ID
- Email domain

+650B

behavioral events monitored annually across the entire Identity Affirmation platform

66%

of attacks in 2020 had bad-reputation IPs, flagged by the consortium, proving its benefits

netStudio

An Indra company

Risk Rules management - Example

The attack triggered the following scores

Account Attack (+100)	Email Domain Risk	Net Anomaly User Agent
Account Harvesting	**Expected location** (-100)	No Widget IP and No JS Key
Account Reputation	Generic Headless Browser	One Hour Login Failure Ratio
Account Testing	Geo Anonymous	Proxy Concealed
Billing Shipping Postal Code Mismatch	**Input Anomaly** (+100)	Proxy Open User Concealed
Browser Age	Input Anomaly Key	Purchase Event Velocity
Credit Card Testing	Input GUI	**Risky IP** (+100)
Credit Card Sharing	Input Replay	Scripted Known Bot
Credit Card Velocity	Input Scripted	TOR exit node
Device Event Velocity (+100)	IP Reputation	Impossible user agent
Device Fingerprint Reputation	Login Failure Ratio	**Viable user agent** (-150)
Device Reputation	Login Failure Ratio Carrier	
Email Anomalous	**Login velocity** (+100)	Attack Score = 250
Email Anonymous	Net Anomaly IP	

green	yellow	red
0 to 99	100 to 199	200+

Policies for the attack

- If score >100 ⟶ Step up
- If score >200 ⟶ Block
- If traffic from <risky country> ⟶ Block
- If Device is new ⟶ Step up

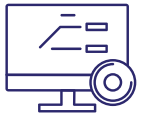
Implementing Identity affirmation

30 DAY TUNING PERIOD

Identity affirmation requires a 30 day tuning period after going live to observe traffic patterns and create an accurate model.

INITIAL 30 DAY TRAFFIC REPORT

We send out a 30 day traffic report summarising patterns and the types of signals and attacks we see.



DASHBOARD REVIEW

We take clients through the Identity affirmation dashboard and explore the functionalities of the application.

FRAUD FEEDBACK

We encourage clients to provide fraud examples or files to help tune the Identity affirmation ruleset.

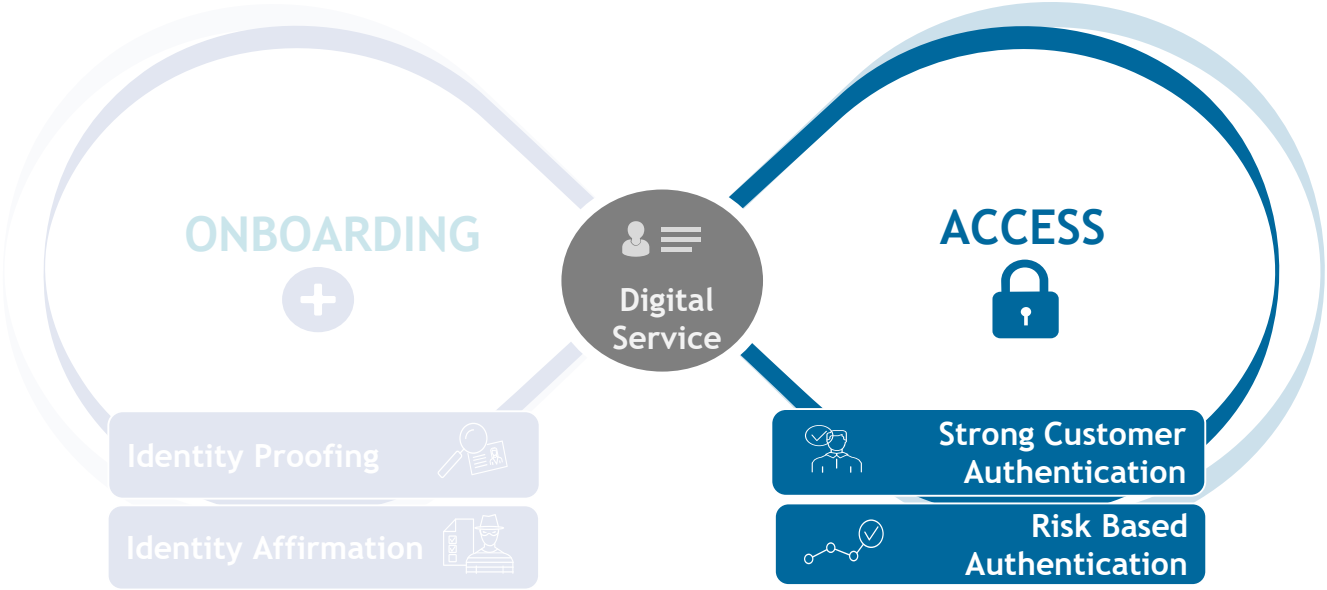
AUTOMATED ATTACK REPORTING

We provide daily traffic reports when high volume attacks are observed.

Using a Digital Identity

About Authentication

The journey loop



ORCHESTRATION

FRICTIONLESS USER EXPERIENCE

ENHANCED SECURITY

REGULATORY COMPLIANCE

netStudio

An Indra company

Password problems

THREAT

‘123456789’
‘password’

Still Most popular passwords in 2020

81%

Data breaches related with weak or stolen passwords

COST

20-50%

Helpdesk calls are password related

HASSLE

130

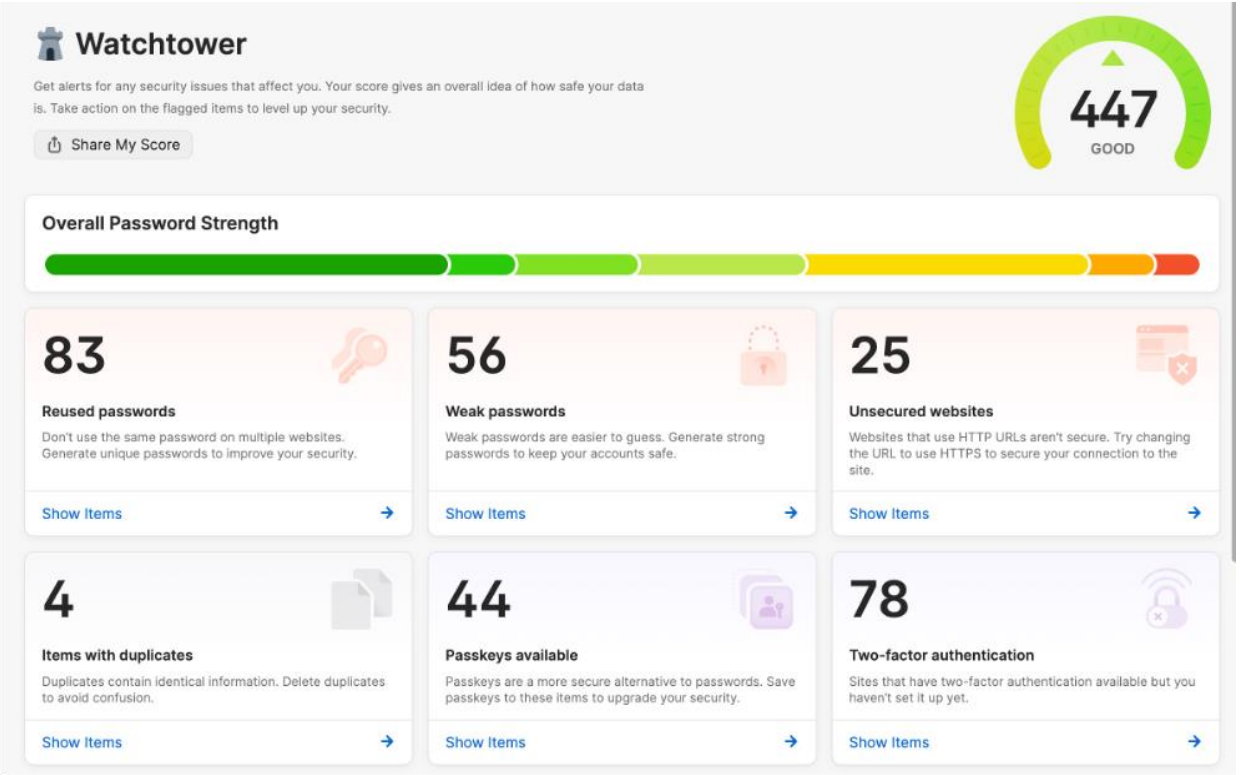
Accounts associated with an email address

50-80%

Users reuse password across accounts

netStudio
An Indra company

Password problems



Gartner:

“A passwordless authentication method is simply one that uses any credential or combination of credentials and signals - that ***doesn’t include a password.”***

When our primary factor is passwords…

81% of hacking-related breaches are caused by weak or stolen passwords (Ping Identity)

43% Gave up on a purchase because they forgot their password (FIDO Alliance)

76% Rise in direct financial loss from successful phishing attacks from 2022-2023 (Proofpoint)

64% either using weak passwords or repeat variations of passwords (Keeper)

Easily phished or socially engineered, difficult to use and maintain

Passkeys

Accelerating the Availability of Simpler, Stronger Passwordless Sign-Ins

Passkey

/ˈpasˌkē/
noun
A FIDO Authentication credential that provides passwordless sign-ins to online services.

A passkey may be synced across a secure cloud so that it's readily available on all of a user's devices, or it can be bound to a dedicated device such as a FIDO Security Key.

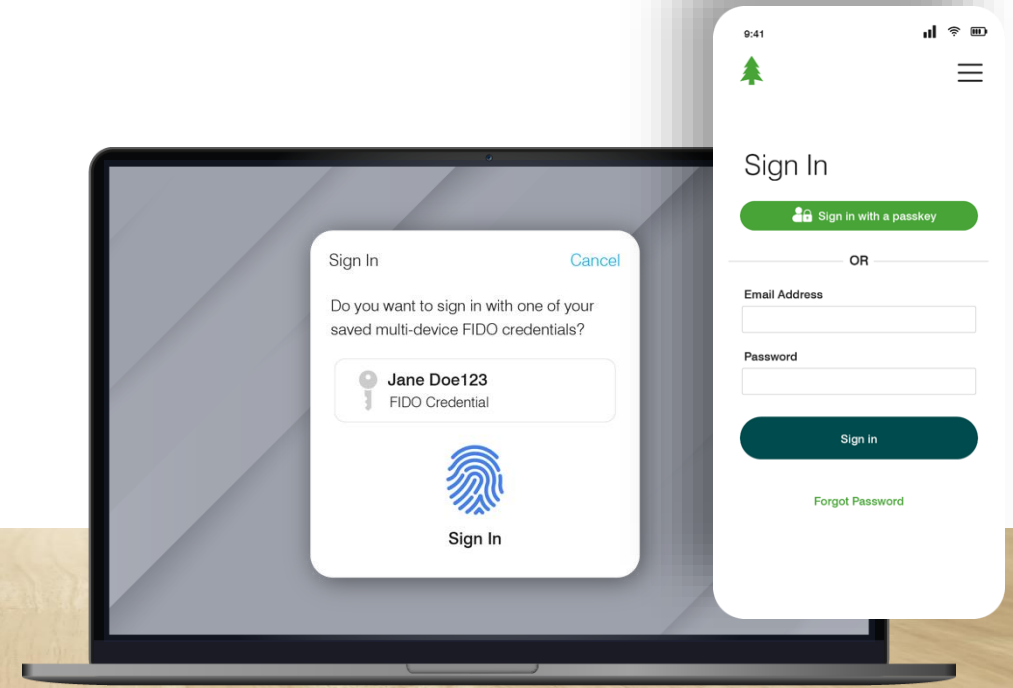
netStudio

An Indra company

Passkeys - paving the way for Passwordless

The **consumer** perspective

Passkeys replace all my passwords and work across my devices



What are passkeys?
The **industry** perspective

aetna amazon AMERICAN EXPRESS arm Bank of America

egis FACEBOOK FEITIAN WE BUILD SECURITY Google HYPR IDEMIA Infineon

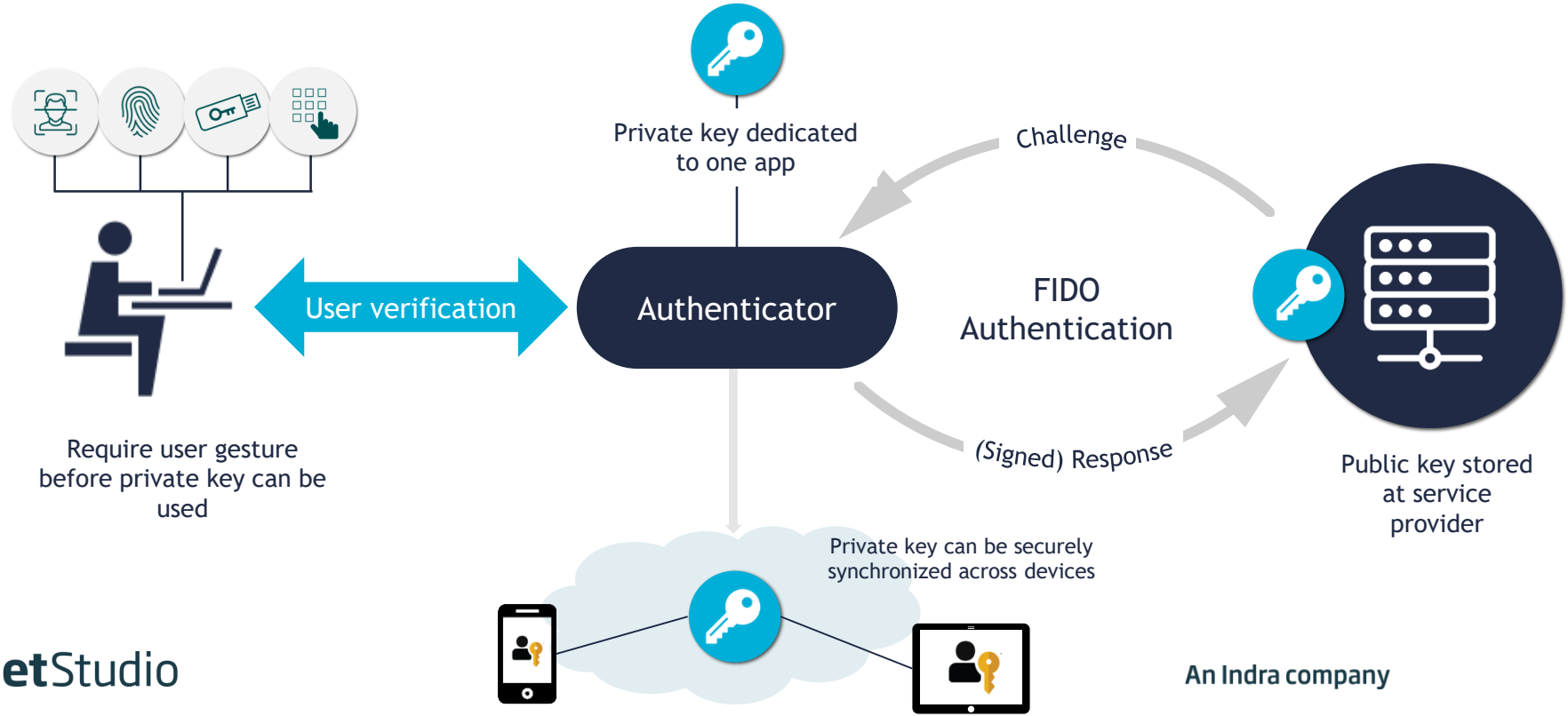
ING intel JUMIO Lenovo LINE LastPass mastercard

Microsoft nok nok docomo OneSpan onfido PayPal QUALCOMM

RAON SECURE RSA SAMSUNG Synaptics THALES transmit TRUSTKEY

USAA VISA vmware WELLS FARGO YAHOO! JAPAN yubico

Same approach – with new syncing capabilities



netStudio

An Indra company

The many benefits of passkeys

UX

> **Biometrics** vs typing

> **Nothing to remember**, renew, reset, re-enrol

Security

> Passkeys are **immune to**:

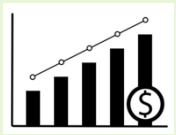
Phishing

Data leaks

ROI

> **More user engagement**

- Faster logins, better UX, less abandonment



> **Less Costs**

- **20-50%** of all helpdesk calls are for password reset*
- **$70** is the average cost of a password reset helpdesk call**

*Source: Gartner
**Source: Forrester

netStudio

An Indra company

Passkeys - Tailored for Regulated industries

Passkeys – Essentials

Synced passkeys are exported to the cloud and propagate to other devices

Passkeys – Enhanced

Managed by
the Mobile App

The private key never leaves the device

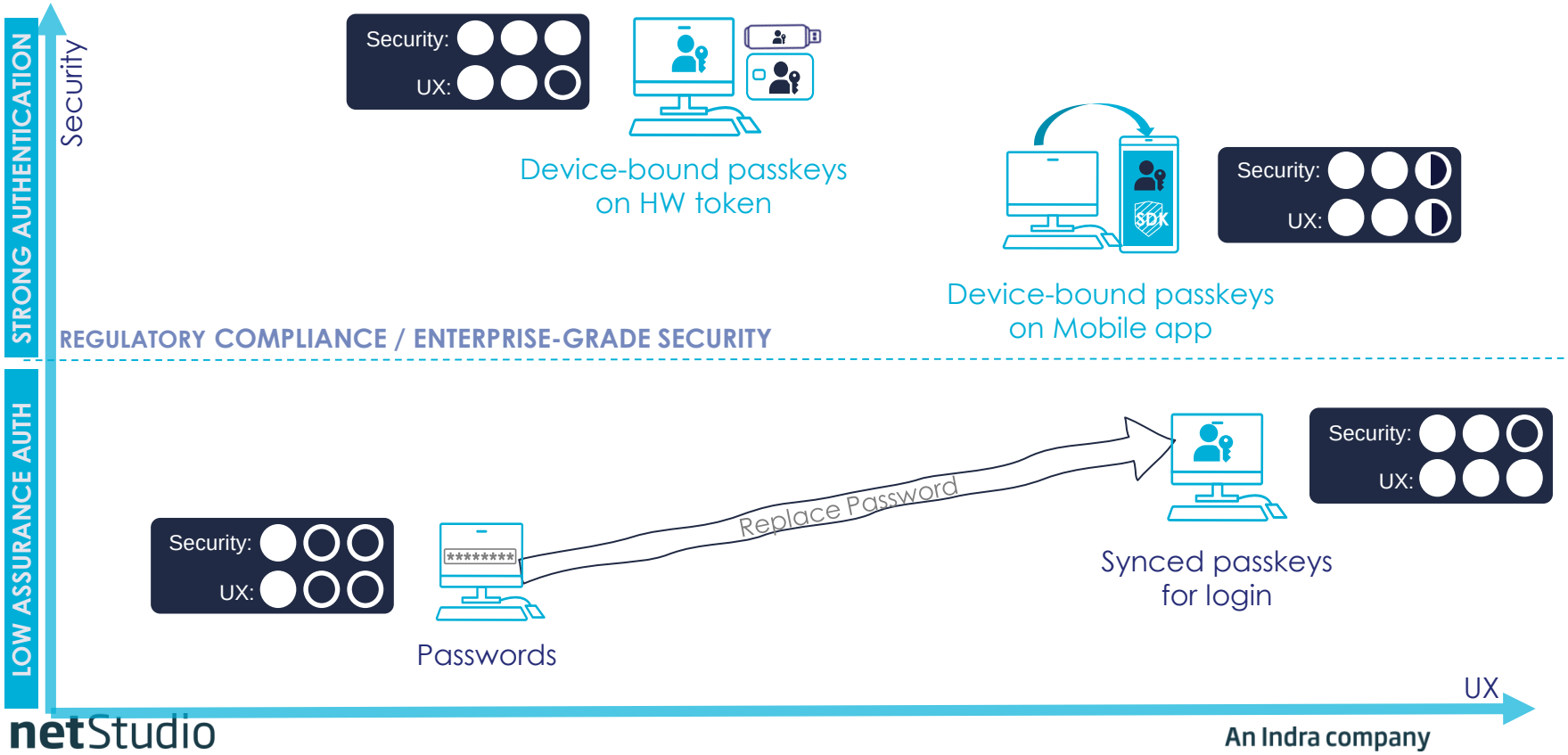
Great for Password Replacement

Great for MFA/SCA

netStudio

An Indra company

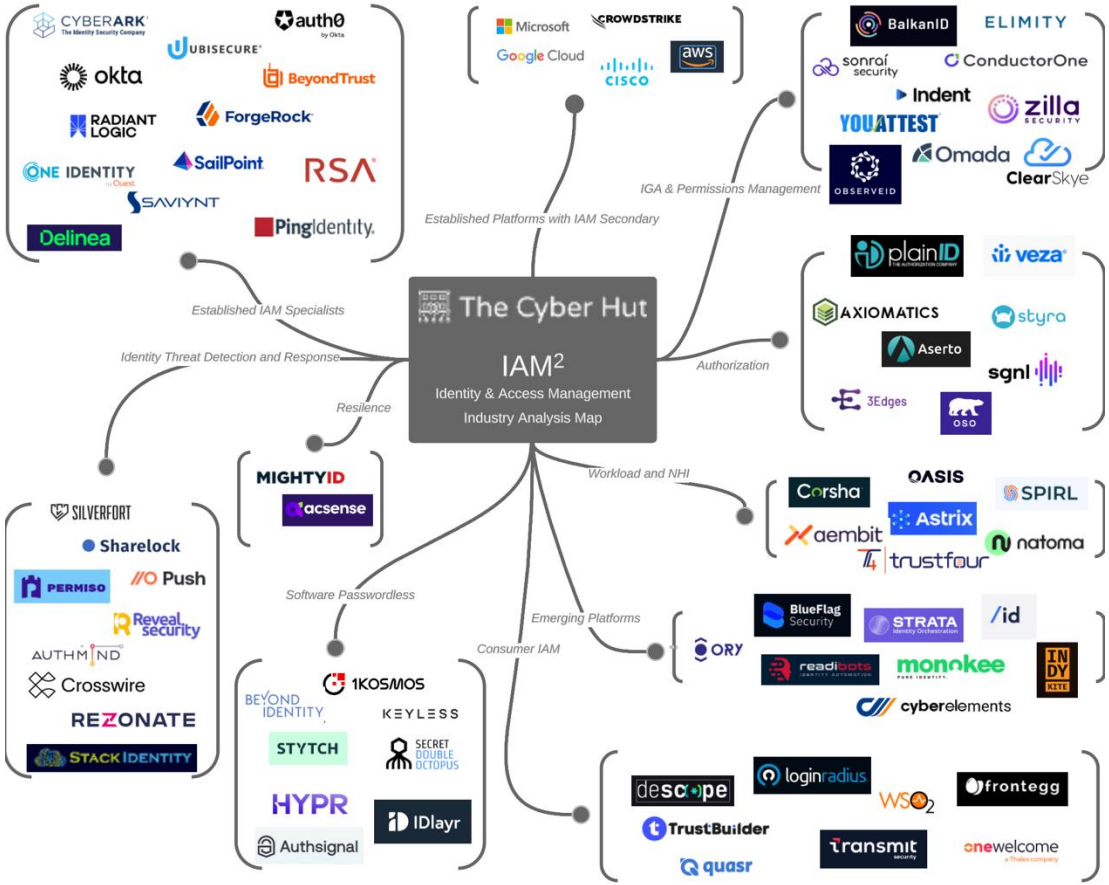
Passkeys for passwords replacement and for SCA



Evolution in the Digital Identity world

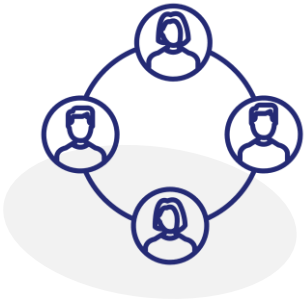
Identity Market 2024

by The Cyber Hut

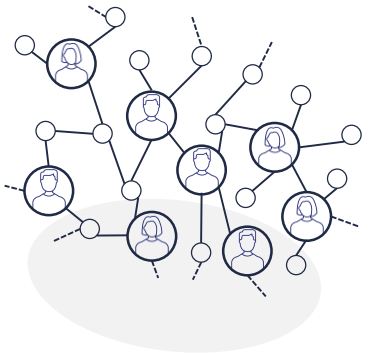


Identity management is evolving

Centralized

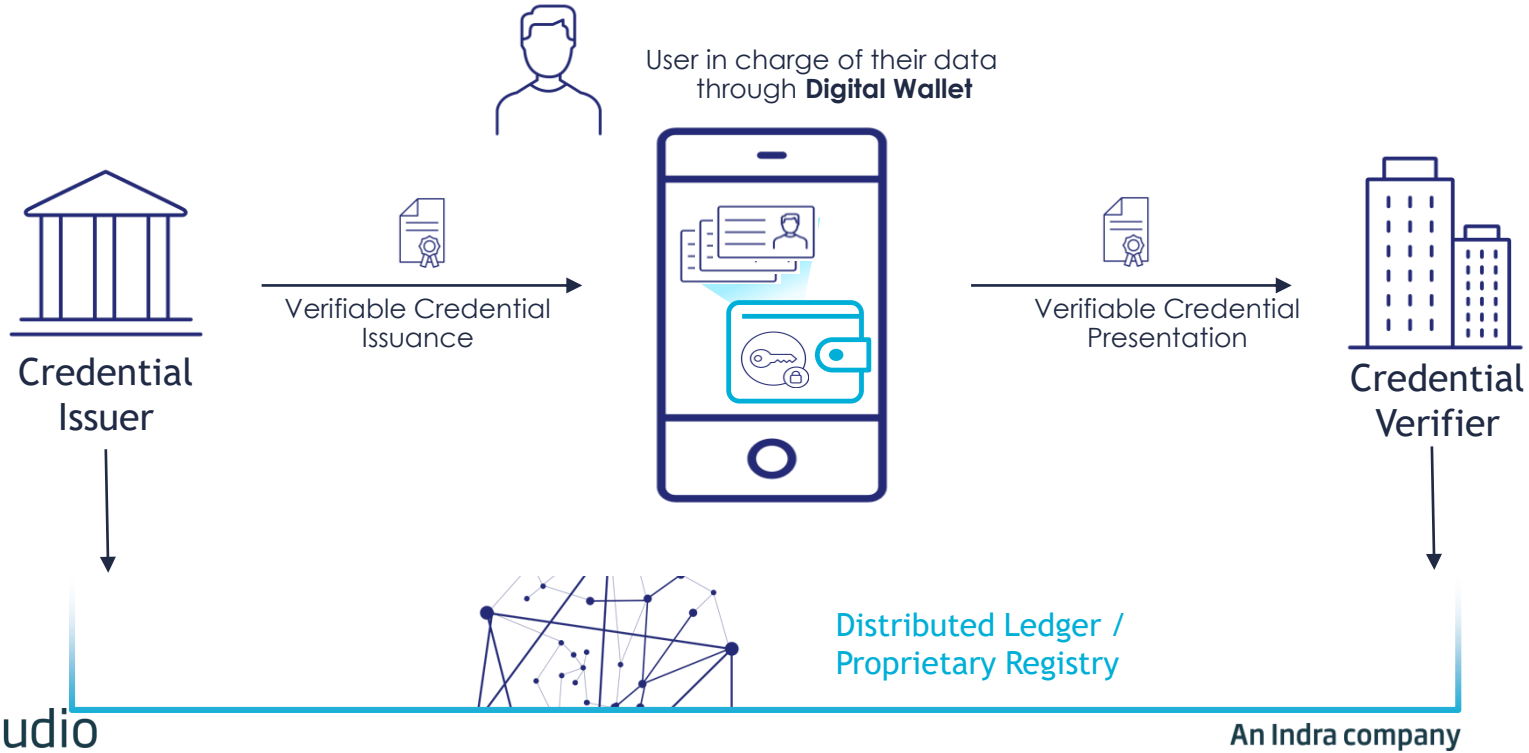


Federated



Decentralized

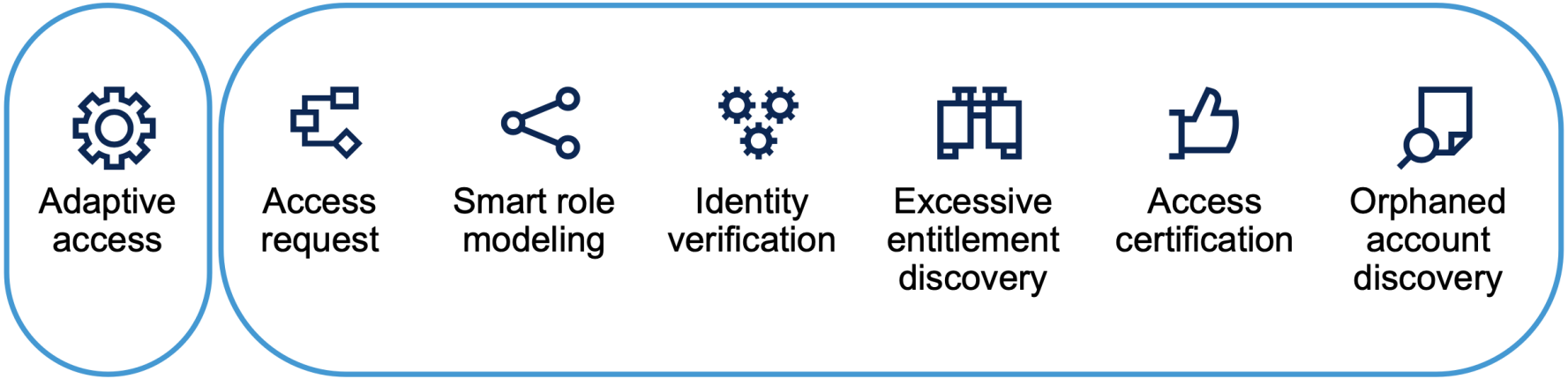
Concept of Self-Sovereign Identity



netStudio

An Indra company

Machine-Learning-Enabled Identity Analytics



Gartner

Q&A

netStudio

An Indra company

BEYOND CYBERSECURITY

Application fraud: fraudsters use a large variety of threat techniques

Phishing/Social engineering
Steal personal data from a user

MitM, key logger, fake website

Spoofing
Masquerade IP/Device identifiers

Virtual machine, proxy, VPN

Scripted attacks
Deploy automation tools

Bots, botnets, hybrid attacks

Human-driven attacks
Workers who bypass bot-mitigation tools

Human farms

Objectives

Synthetic identity

Combines real and fake information to create a new identity

Identity theft

Use a real user's full identity

Mule account

Launder money, obtain credit, transfer money stolen from other accounts