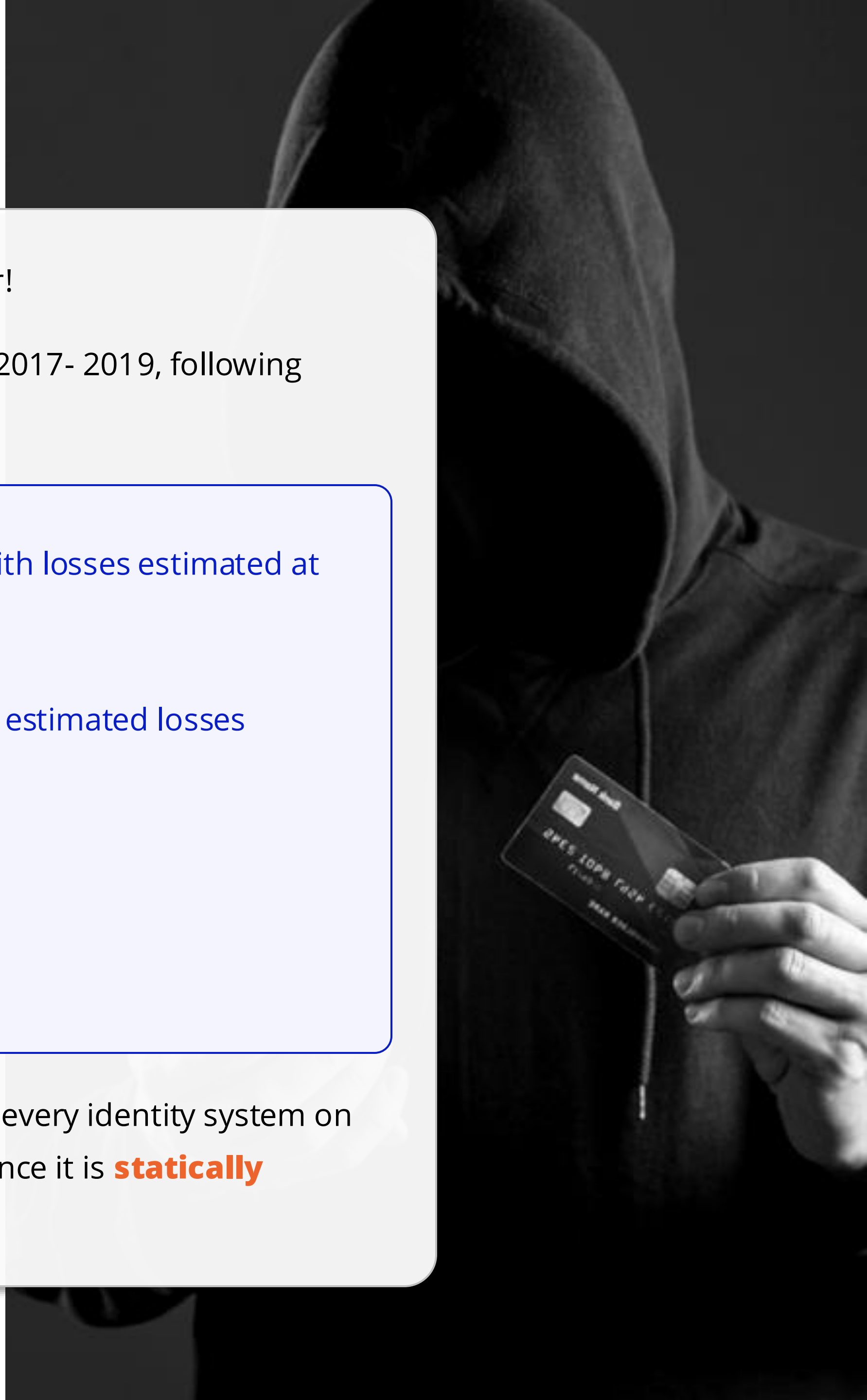
10S Technologies

Dynamic Partial ID

Payment Industry

April 2025

Background

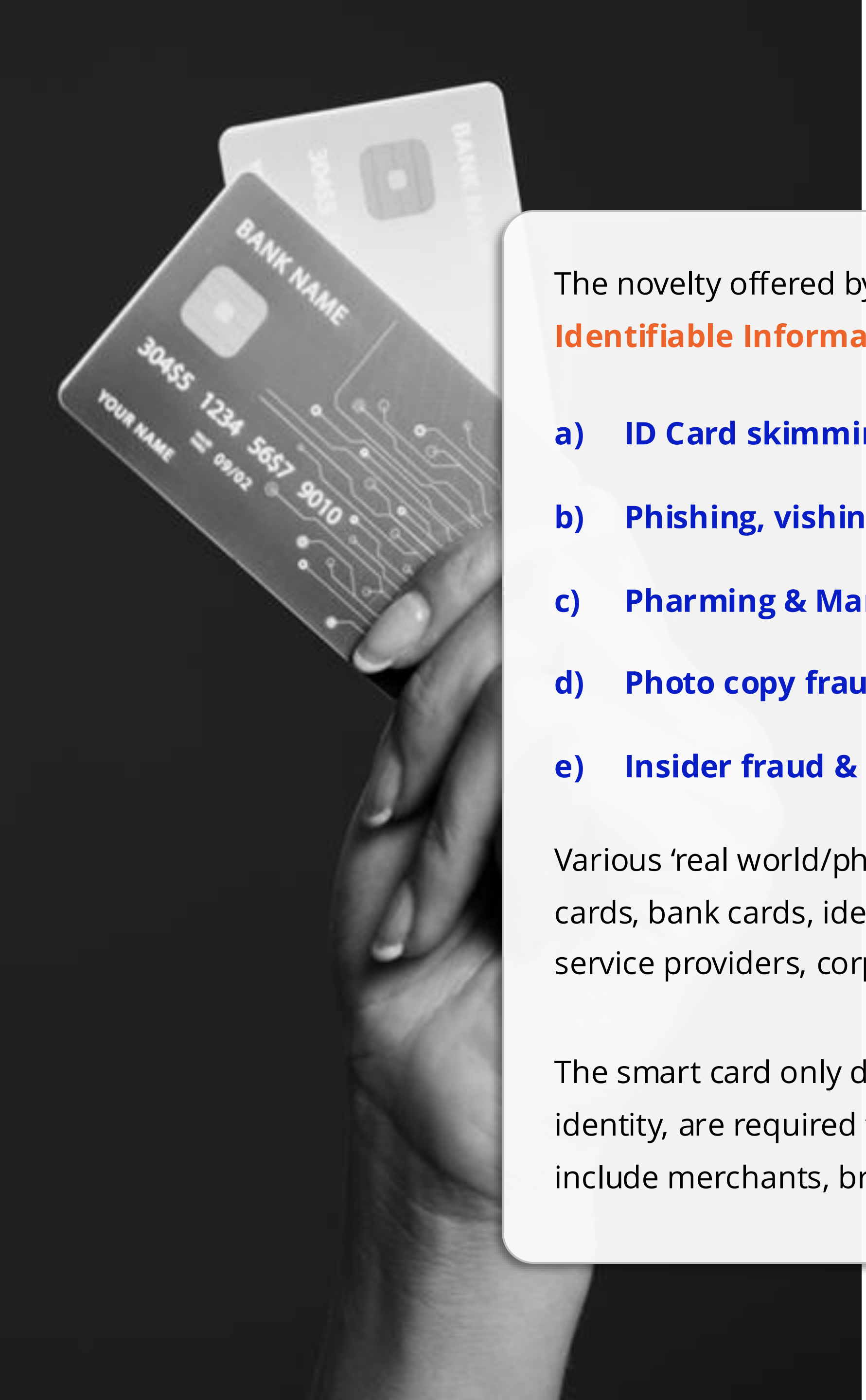


Globally, identity fraud costs people, businesses, and governments more than USD 1 trillion each year!

As per European Commission **study** on online identity theft and identity-related crime, in the period 2017- 2019, following statistics were observed:

- **148 million** EU citizens reported having been targets or victims of different forms of phishing with losses estimated at **EUR 27.0 billion**.
- **32 millions** citizens experienced or had been a victim of bank card or online banking fraud with estimated losses between EUR 882.0 million and 2.4 billion.
- Estimated indirect costs to citizens as a result of identity theft is **EUR 31 billion**.
- Cost of credential theft is about **EUR 400,000** per company.

An examination of multiple fraudulent situations & attack vectors reveals a fundamental weakness in every identity system on the planet - the sensitive Personally Identifiable Information (PII) about an individual is **immutable** since it is **statically printed** on the ID card for an extended period of time.



Introduction

The novelty offered by this patent pending technique relates to safeguarding PII by offering **Dynamic Personally Identifiable Information (DPII)** which completely eliminates static PII & cannot be compromised by means of:

a) **ID Card skimming & social engineering fraud.**

b) **Phishing, vishing & smishing.**

c) **Pharming & Man-In-The-Middle (MITM).**

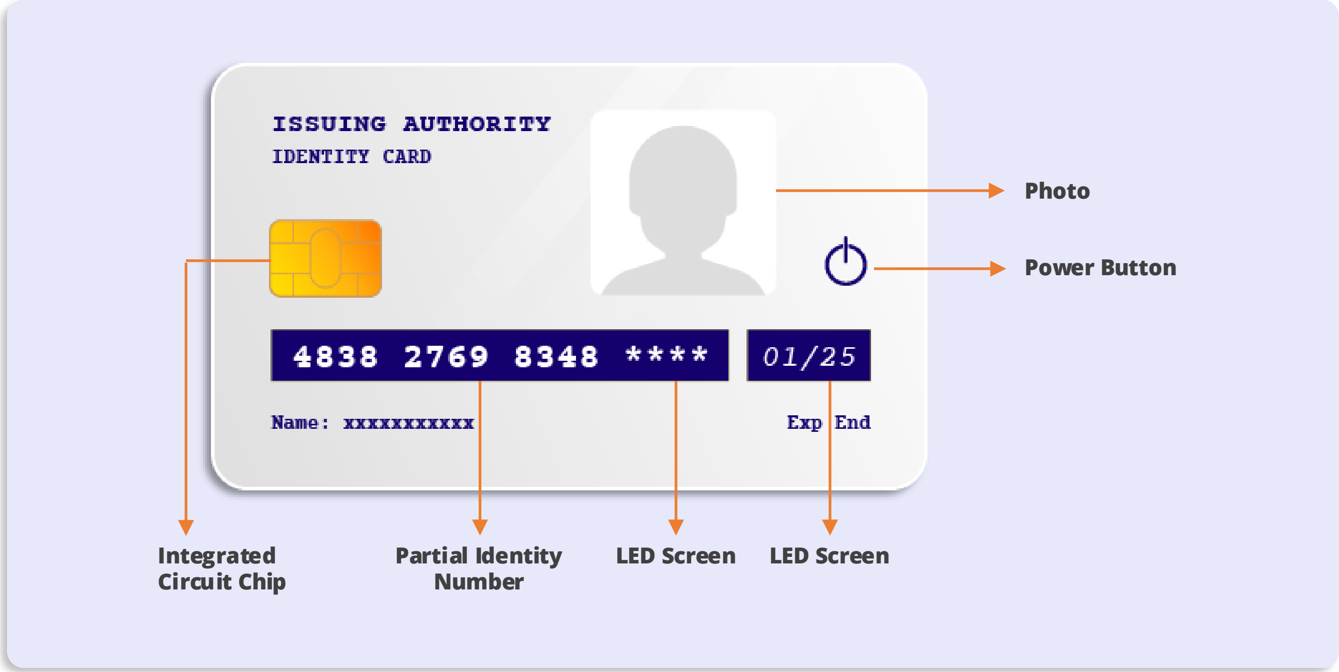
d) **Photo copy fraud & attack.**

e) **Insider fraud & Database breach etc.**

Various 'real world/physical' and 'online' identities can be protected for example passports, driving licenses, national ID cards, bank cards, identity wallets, Username/password etc. Examples of Issuing Authorities are government departments, service providers, corporates, banks etc.

The smart card only displays **'Partial Identity'**. All relying parties (RP) and potential attackers who need to consume the identity, are required to authenticate to the Identity Provider to fetch the **'Complete Identity'**. Examples of relying parties include merchants, brokers, security officer, service provider applications etc.

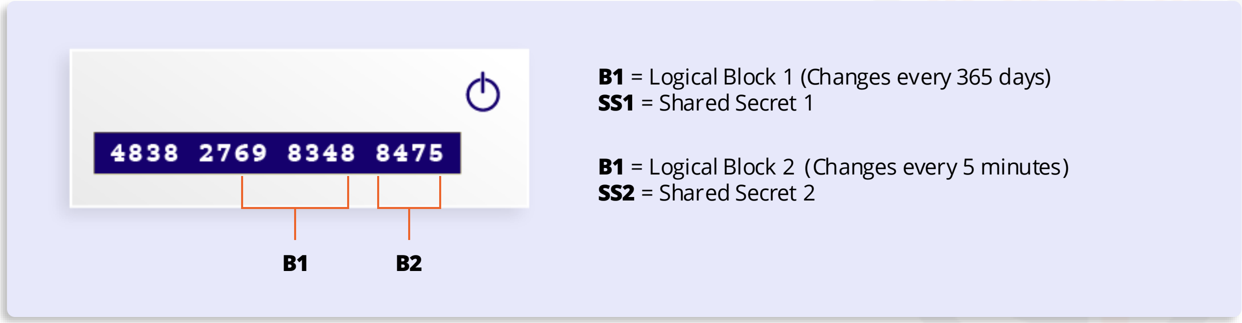
Description



The proposed identity card would have a dynamic identity number & card expiry displayed on LED screen - banks cards will have dynamic security code as well. These values will renew as often as the Issuing Authority determines.

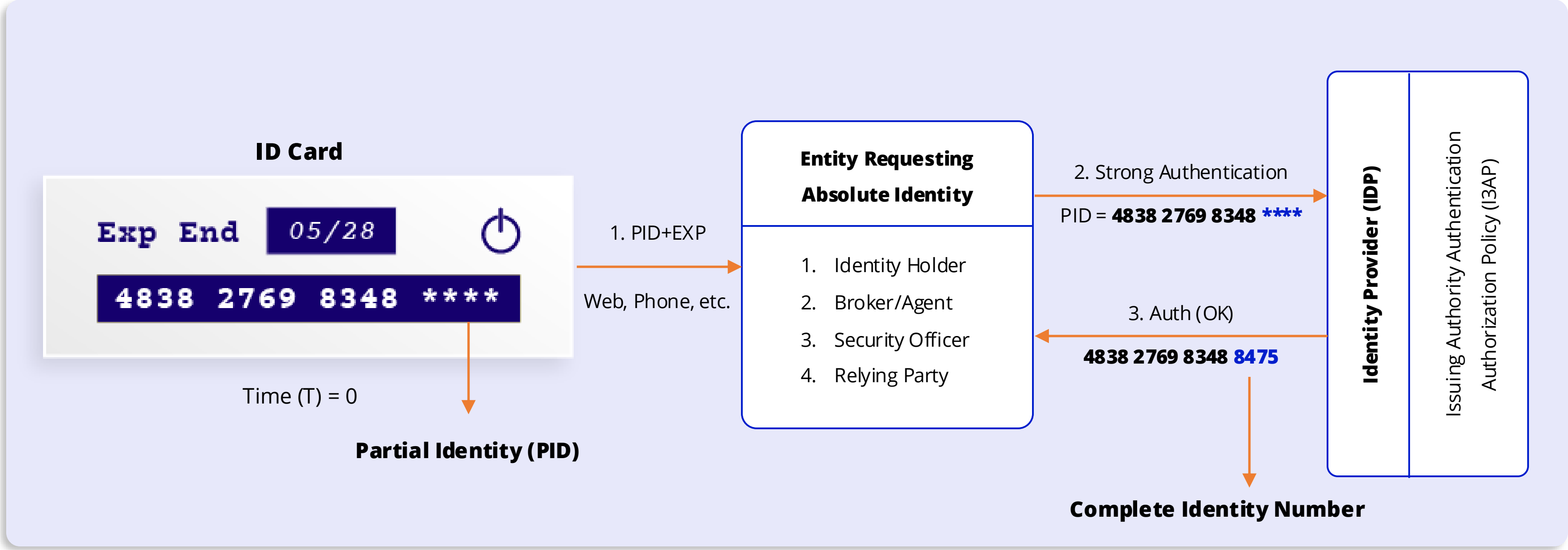
One of the system's innovations and a key distinction is that the ID card won't display the entire identity number.
Rather, a **Partial Identity Number (PID)** is displayed, for example 4838 2769 8348 ****.

The identity number on the suggested smart card will be divided into two or more logical blocks say B1 and B2. The time intervals, after which these block values change, as an example, are B1 (1 year), B2 (5 minutes). A shared secret (SS) key corresponds to each of the logical blocks and is stored securely in smart card and IDP database.



B1 = Logical Block 1 (Changes every 365 days)
SS1 = Shared Secret 1

B1 = Logical Block 2 (Changes every 5 minutes)
SS2 = Shared Secret 2



* Refer foot notes for detailed authentication flow

* For details of logical block association with shared secrets and steps to generate PID by the smart card and IDP, refer **Whitepaper** (page #8).

At T=5 min, the complete identity returned by IDP has changed – 4838 2769 8348 0076. Renewable identities!

Partial Identity (PID) & One Time Complete Identity (OTCI)

T=0 min, PID = 4838 2769 8348 * & OTCI returned = 4838 2769 8348 8475***

T=5 min, PID = 4838 2769 8348 * & OTCI returned = 4838 2769 8348 0076***

In this example, pre-configured time interval is five minutes. Because the identity number returned only appears once, it goes by the name **One Time Complete Identity (OTCI).** These unique OTCIs are tied to respective Relying Parties who consume these identities.

The process of Relying Party authenticating to IDP comes in two flavours

a) Natural Person **b) Machine-to-Machine**

Issuing Authority Authentication Authorization Policies (I3AP) can **1)** prohibit any natural person from obtaining the OTCI, **2)** allow Identity Holder Consent for OTCI/CID fetch by RPs, **3)** allow contact based or contactless transaction, **4)** PIN or biometric based Mobile App Authentication mode, **5)** PID and Expiry Date Synchronization, **6)** time interval after which the identity number (OTCI) will change & **7)** allowed incorrect PID attempts.

One-Time Partial Identity (OTPI) embodiment provides an effective way for the issuing authority to do away with PID caching. The identity card will include one extra logical block, B3, rather than two blocks B1 and B2. The time intervals, as an example, are B1 (1 year), B2 (5 minutes), and B3 (5 minutes). By design, B1 and B2 values are always displayed when the end user pushes the button, while B3 is obfuscated, as shown below.

One-Time Partial Identity (OTPI) & One Time Complete Identity (OTCI)

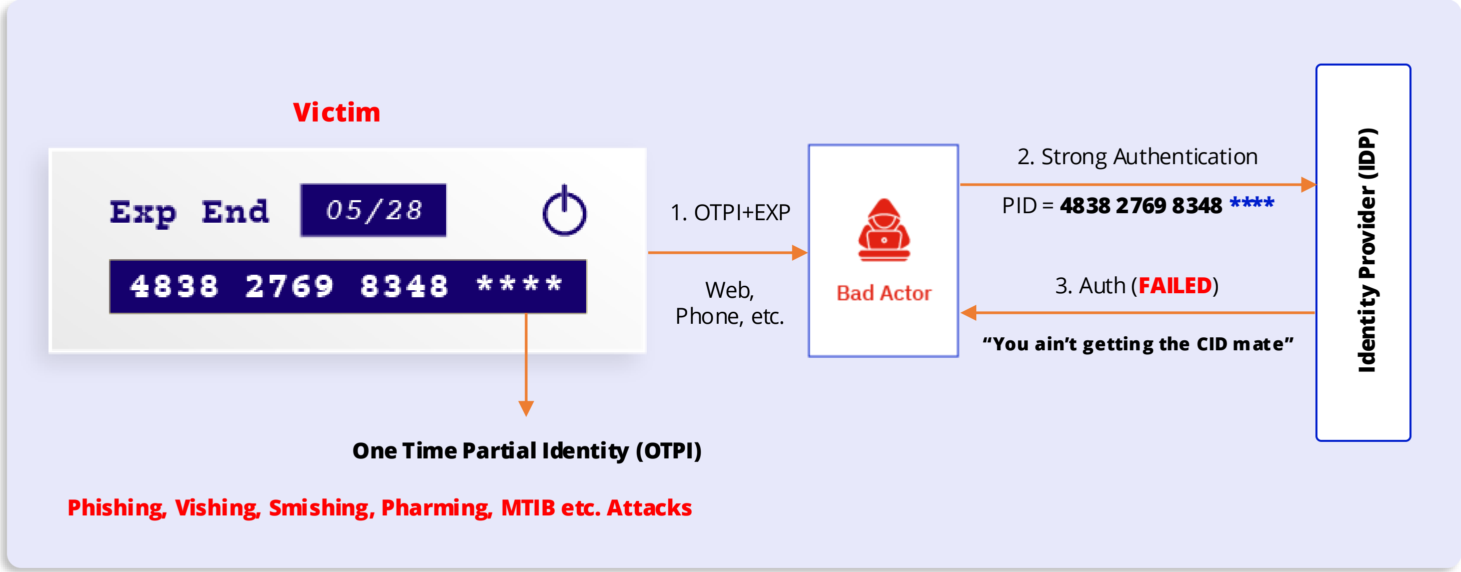
T=0 min, OTPI = 5849 3979 6061 278 ** 4 & OTCI returned = 5849 3979 6061 278 55 4

T=5 min, OTPI = 5849 3979 6061 201 ** 4 & OTCI returned = 5849 3979 6061 201 37 4

T=10 min, OTPI = 5849 3979 6061 203 ** 4 & OTCI returned = 5849 3979 6061 203 64 4

The term One Time Partial Identity (OTPI) comes from the fact that the PID shown is dynamic, time-bound, partial and only produced once. The main benefit of OTPI is that it provides a truly dynamic partial identity, making it impossible for anyone—even malicious actors to cache them.

MITM Mitigation and Threat


Victim
Exp End
05/28
4838 2769 8348 ****
1. OTPI+EXP
Web,
Phone, etc.
Bad Actor
2. Strong Authentication
PID = 4838 2769 8348 ****
3. Auth (FAILED)
"You ain't getting the CID mate"
Identity Provider (IDP)
One Time Partial Identity (OTPI)
Phishing, Vishing, Smishing, Pharming, MTIB etc. Attacks

* Refer foot notes for authentication flow

The OTCI will be linked to the ID of the RP. In the event of inside fraud, IDP will revoke this RP ID as soon as the incident is reported thus guaranteeing that future fraud is avoided by same fraudster. The technique can be used to secure online identities as well. The following mechanisms are available for use

a) The PID can act as Username. This way, the users will not have to remember their username.

b) OTPI produces 'dynamic usernames' or One Time User Name (OTUN). We can completely eliminate username as an attack vector.

c) Expiry date can serve as a dynamic password.

Advantages of Dynamic Partial Identity

1. The technique offers **Dynamic Personally Identifiable Information (DPII).**
2. DPII **defends against various identity attacks such as** Identity skimming fraud, phishing, vishing, smising, MITM, pharming, replay attack, key logger, malware browser memory attack, brute force, Fraudulent Admin, database breach, Social Engineering, photocopy fraud and MFA vulnerabilities.
3. In order to accommodate different needs & the security posture of various issuing authorities, the technique allows a **range of options** like One Time Identity (OTI), Partial Identity (PID), One Time Partial Identity (OTPI), Complete Identity (CID) and One Time Complete Identity (OTCI).
4. Numerous I3AP policies are available and can be configured in **real-time**, thus offering flexibly.
5. Sensitive mutable PII is automatically reset by short lived identities (OTCI) in the service provider database. This includes: a) identifiers, such as health insurance, patient, employee, student ID numbers, Bank Card numbers etc. and b) the expiration date of the identity. This greatly **addresses privacy concerns**.
6. A particular end-user OTCI may only be utilised by a single, distinct relying party. Its greatest benefit is the ability to cope with **PII misuse** efficiently.
7. This concept is broad-spectrum & can secure both **physical** & **online** identities.

Advantages - Cont...

8. There is **no need for end-user education** or awareness campaigns warning users not to share sensitive personal information.

9. The system is **not invasive** and does not drastically alter users' conduct.

10. Regarding strong 2FA, apart from dynamic passwords, this technique also offers **dynamic Usernames** – One Time Username (OTUN)!

11. Through identity federation, identity issued by one issuing authority (for example National ID) can be used by other relying parties (banks, corporates etc.) This can be an **additional source of revenue** for issuing authorities!

12. Issuing authorities will significantly **reduce logistical costs** since there will be no need to reissue and ship cards because of their expiration.

13. With secure hardware smart cards, the technique will be able to offer 3-factor authentication and will fend off malware attacks like **Pegasus** etc.

Identity Threats and Mitigation Matrix

Threat	Description	Mitigation
Identity Skimming	A fraudster somehow gets victim’s ID card details, which can be misused later.	**Yes**
Man-in-the-Middle	The attacker intercepts the credentials and data while they are in transit.	**Yes**
Phishing, Vishing, Smishing	The attacker targets unsophisticated users and fools them into entering their card details into a fake web site.	**Yes**
Pharming	The attacker poisons the DNS server & redirects users to the fraudulent web site.	**Yes**
Replay Attack	The attacker records a copy of the identity information & replays it at a later time to perpetrate identity theft.	**Yes**
Key Logger	This malware records all keystrokes & mouse clicks & relays information to the criminal.	**Yes**
Malware Browser Memory Attack	The attacker attempts to find the credentials in the memory of a system.	**Yes**
Brute Force	Attacker exhaustively attempts all possible combination of missing identity data, which eventually leads to guessing the correct one.	**Yes**
Fraudulent Admin/Database Breach	A fraudulent administrator gets access to PII and misuses it. It is true in case of a database breach as well.	**Yes**
Social Engineering	While the ID card is being used, a fraudster tries to peek over the victim's shoulder to acquire identity information or leverage covert cameras to record it.	**Yes**
Photocopy Fraud	When a victim needs to avail a specific service, they give a photocopy of their identity card, which can be misused.	**Yes**
Multi Factor Authentication Vulnerability	Authentication attacks commence from identifying victim’s username, which is always static.	**Yes**

* Refer **Datasheet** or **Whitepaper** (Identity Threats & Mitigation Matrix) for detailed explanation.

Virtual Card Competitive Analysis

Pros

Virtual Card Prevents against following attacks:

1. Identity Skimming
2. Reply Attack
3. Fraudulent Admin/Inside Fraud/DB Breach
4. Social Engineering

Cons

Virtual Card does NOT prevent against following attacks, since victim can still be tricked into sharing virtual card details with a fraudster:-

1. MITM
2. Phishing/Smishing/Vishing
3. Pharming
4. End user has to be online. Sometimes it's a challenge.
5. No online net banking protection

DPID vs Payment Cards Competitive Analysis

Type ID		Payment Cards		Dynamic Partial ID	
Form Factor		Physical	Virtual	Physical	Virtual
Threat	Description	Threat Mitigation			
Card Skimming	A fraudster gets victims' ID details via skimming devices (NCF/RFID), hidden cameras etc. followed by data extraction. This data is misused later.	No	Yes	Yes	Yes
Man-in-the-Middle	The attacker intercepts the card details while they are in transit (e.g. weak Wi-Fi). In this case, the attacker appears as the relying party to the user and as the user to the target server.	No	<No>	Yes	Yes
Phishing, Vishing, Smishing	The attacker targets unsophisticated and unsuspecting victims and fools them into sharing their card details. The attack is launched via email, website, phone calls or SMS.	No	<No>	Yes	Yes
Pharming	The attacker poisons the DNS server & redirects users to the fraudulent web site. Users do not suspect anything wrong because the user selects the genuine web site from a saved favourite or actually types in the correct URL.	No	<No>	Yes	Yes
Replay Attack	This attack follows from card skimming, MITM, phishing, pharming, inside fraud or DB breach. Compromised (harvested) data is misused (replayed) at a later time to perpetrate identity theft.	No	<No>	Yes	Yes
Key Logger	This malware allows the attacker to record all keystrokes and mouse clicks & regularly transmits the credential information to the criminal via the internet.	No	No	Yes	Yes
Malware browser memory attack	Malware attack targets the credentials downloaded in the memory of a system.	Yes	Yes	Yes	Yes

Competitive Analysis – Cont…

Type ID		Govt IDs		Dynamic PII	
Form Factor		Physical	Virtual	Physical	Virtual
Threat	Description	Threat Mitigation			
Fraudulent Admin or DB breach	A fraudulent administrator gets access to PII on the backend server and misuses it. It is true in case of a database breach as well.	No	<No>	Yes	Yes
Brute Force	Attacker exhaustively attempts all possible combination of missing identity data.	Yes	Yes	Yes	Yes
Social Engineering – Shoulder Surfing	While the ID card is being used, a fraudster tries to peek over the victims' shoulder to acquire card details. An advanced form could be spying by covert cameras.	No	Yes	Yes	Yes
Zero-day Vulnerability	Mobile OS security flaw, for example Pegasus, that is unknown to the OS vendor.	Yes	No	Yes	No
Multi factor Authentication Vulnerability	Does the ID card/system itself enhance online access 2FA?	No	No	Yes	Yes
Photocopy Fraud	When a victim needs to avail a specific service, at time of hotel checking etc. they give a photocopy of their identity card. A dishonest employee could mis use the identity ?	N/A	N/A	Yes	Yes
SIM Swap Attack	A SIM swap attack occurs when Id is linked to SIM & fraudsters convince a telecom provider to transfer a victim's mobile number to a new SIM card that the attacker controls.	<Yes>	<Yes>	Yes	Yes

Competitive Analysis – Cont…

Type ID		Govt IDs		Dynamic PII	
Form Factor		Physical	Virtual	Physical	Virtual
Threat	Description	Threat Mitigation			
User training/Awareness Campaign	Does the ID system by itself secure identity data or it there dependence on user training or awareness?	Yes	No	Yes	Yes
Dependence on smart phone/device	Does the technology by itself self-sufficient to secure identity data? Or there is dependence on smart phone or end user computing device?	Yes	No	Yes	No
Broad-Spectrum	Is there effective coverage across entire public and private sector relying parties? Or is there reliance on legislation to offer robust protection?	Yes	Yes	Yes	Yes
Total Score		**7 / 16**	**6 / 16**	**17 / 17**	**15 / 17**
Percentage		**44%**	**38%**	**100%**	**88%**

LEGEND	**YES - 1 Point**	**NO - 0 POINT**	**N/A**	**<RESPONSE>**	**DATE UPDATED**
DESCRIPTION	**STRENGTH**	**LIMITATION/VULNERABILITY**	**NOT APPLICABLE**	**SCORING MAY CHANGE WITH DIFFERENT TECHNIQUES**	**19th JULY 2025**

Conclusion

- Unlike any other ID system on the planet, this approach provides the broadest protection against all identity threats known to exist.
- Renewable Identity technique constitutes a crucial component of a much broader initiative to develop a **Next-Generation Identity Framework**.
- Apart from directly reducing identity fraud, which costs more than $1 trillion annually, such an identity framework can also indirectly support global economies, which are worth many trillions of dollars. According to **Steve Knack**, trust is worth 99.5% of a country's GDP!

Thank You

10S Technologies