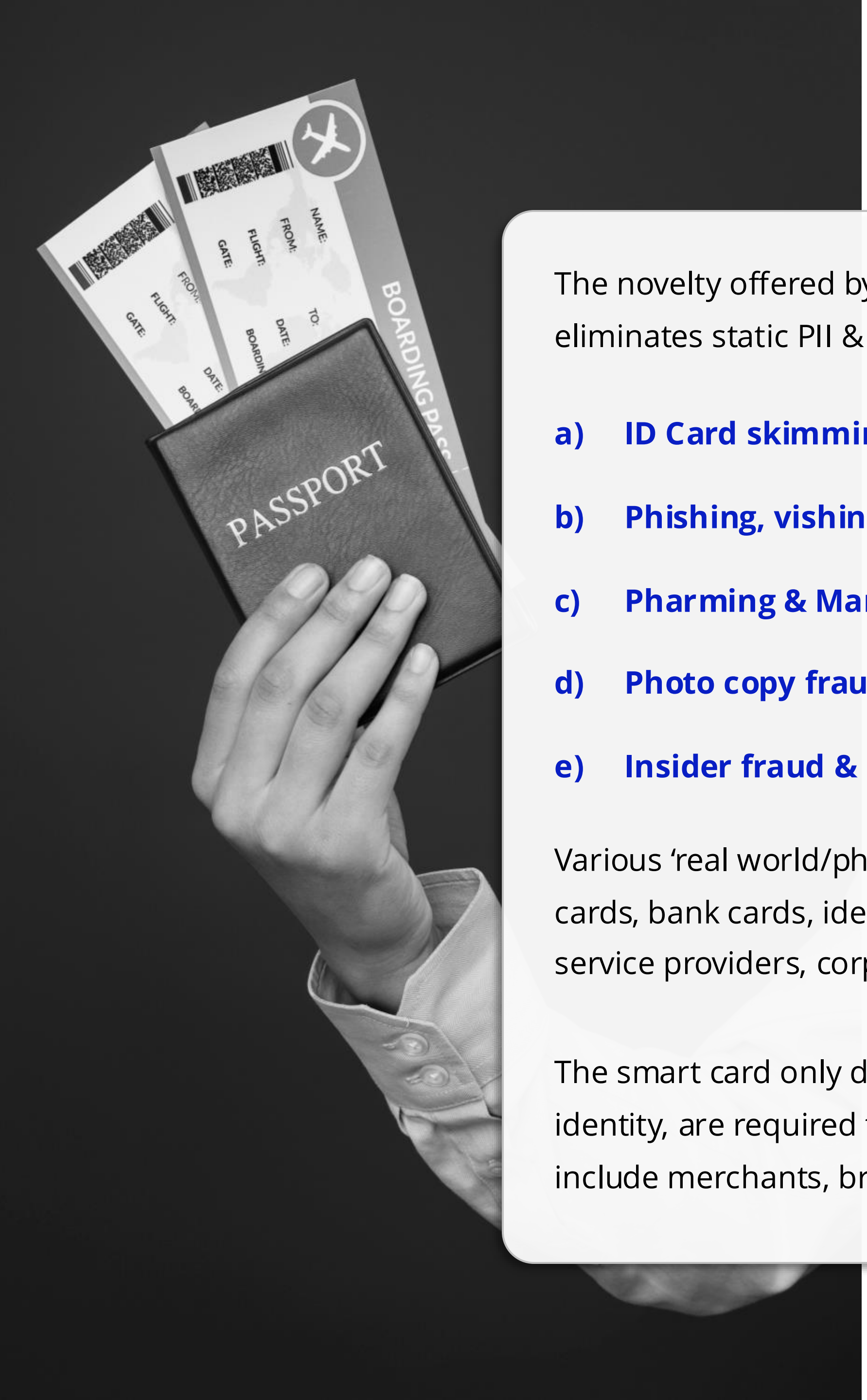
10S Technologies

Āṅśik ID

Dynamic Partial ID

April 2025



Introduction

The novelty offered by this patent pending technique relates to safeguarding PII by offering **Partial ID** 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).**

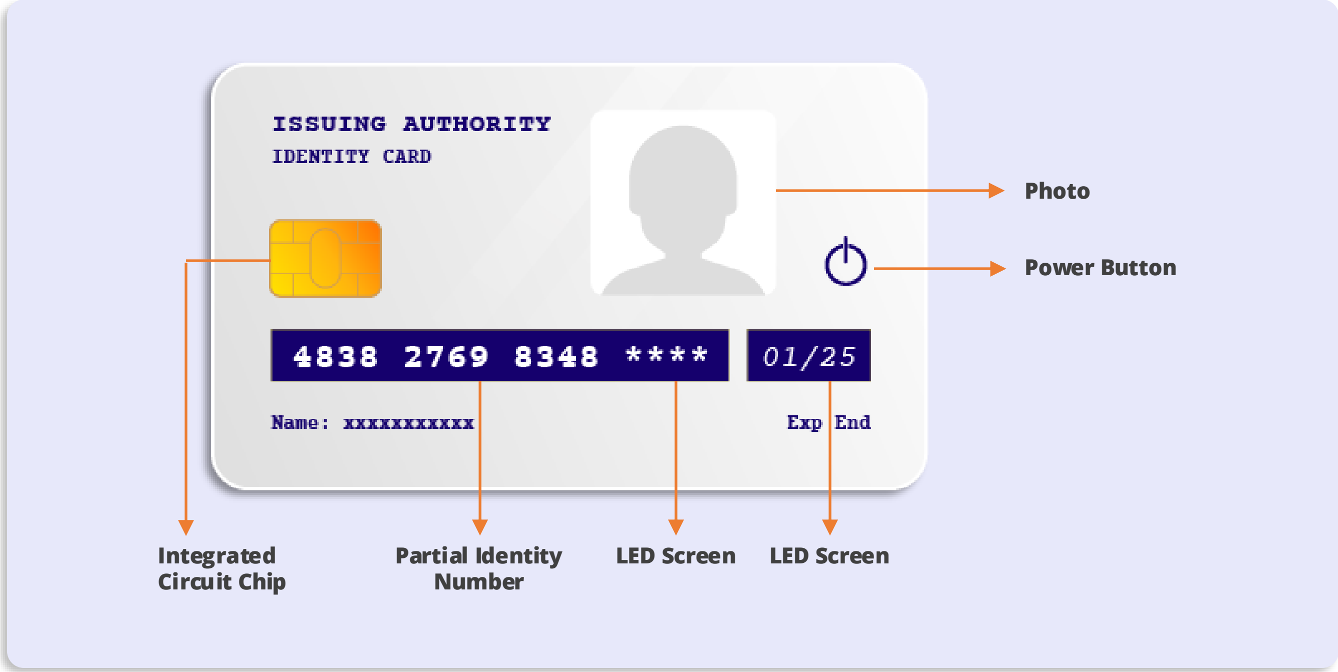
d) **Photo copy fraud & attack.**

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.

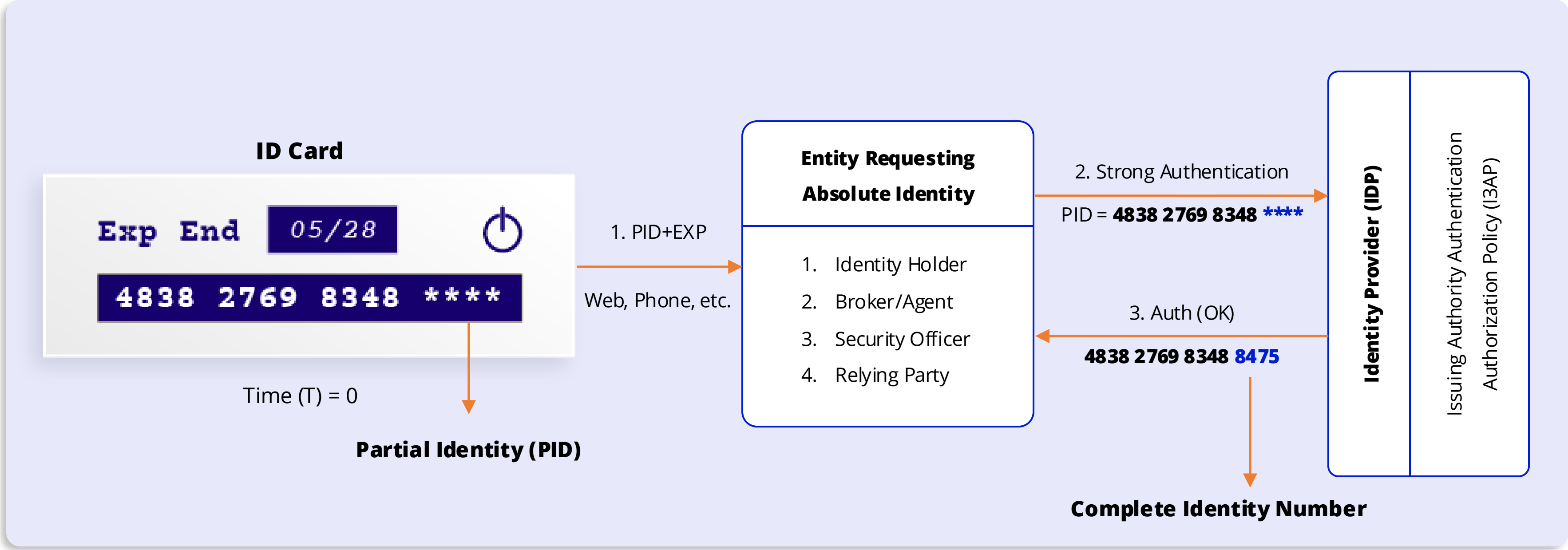
Description



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 ****.

Concept flow...



ID Card

Exp End 05/28

4838 2769 8348 ****

Time (T) = 0

Partial Identity (PID)

1. PID+EXP

Web, Phone, etc.

Entity Requesting Absolute Identity

1. Identity Holder
2. Broker/Agent
3. Security Officer
4. Relying Party

2. Strong Authentication

PID = **4838 2769 8348 ******

3. Auth (OK)

4838 2769 8348 8475

Complete Identity Number

Identity Provider (IDP)

Issuing Authority Authentication Authorization Policy (I3AP)

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***

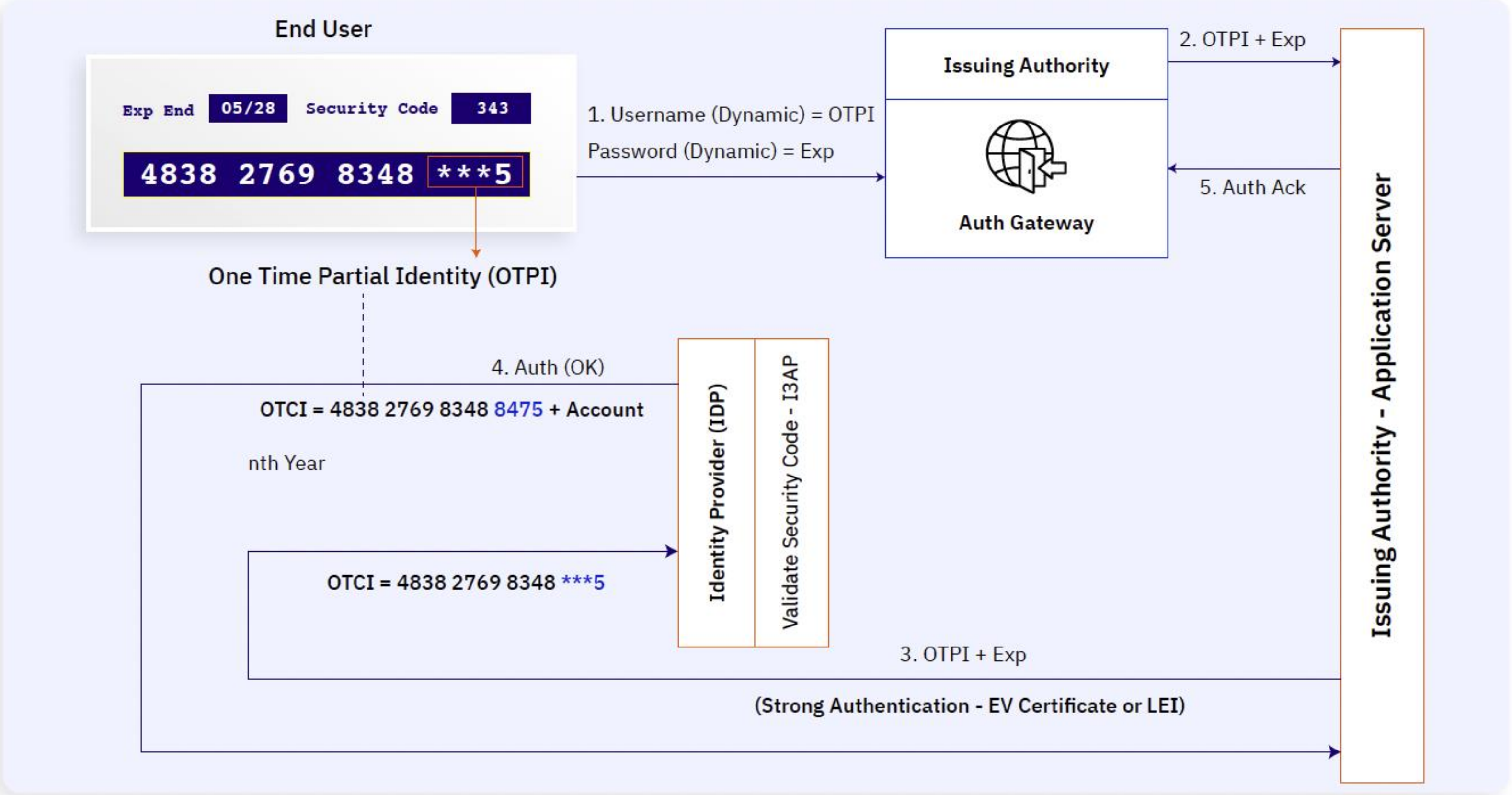
In this example, pre-configured time interval is five minutes. Because the identity number returned only appears once, it goes by the name **One Time Complete Identity (OTCI).** These unique OTCIs are tied to respective Relying Parties who consume these identities.

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.

Online Authentication – 2FA



End User

Exp End 05/28 Security Code 343

4838 2769 8348 ***5

One Time Partial Identity (OTPI)

1. Username (Dynamic) = OTPI

Password (Dynamic) = Exp

Issuing Authority

Auth Gateway

2. OTPI + Exp

5. Auth Ack

Issuing Authority - Application Server

4. Auth (OK)

OTCI = 4838 2769 8348 8475 + Account

nth Year

OTCI = 4838 2769 8348 ***5

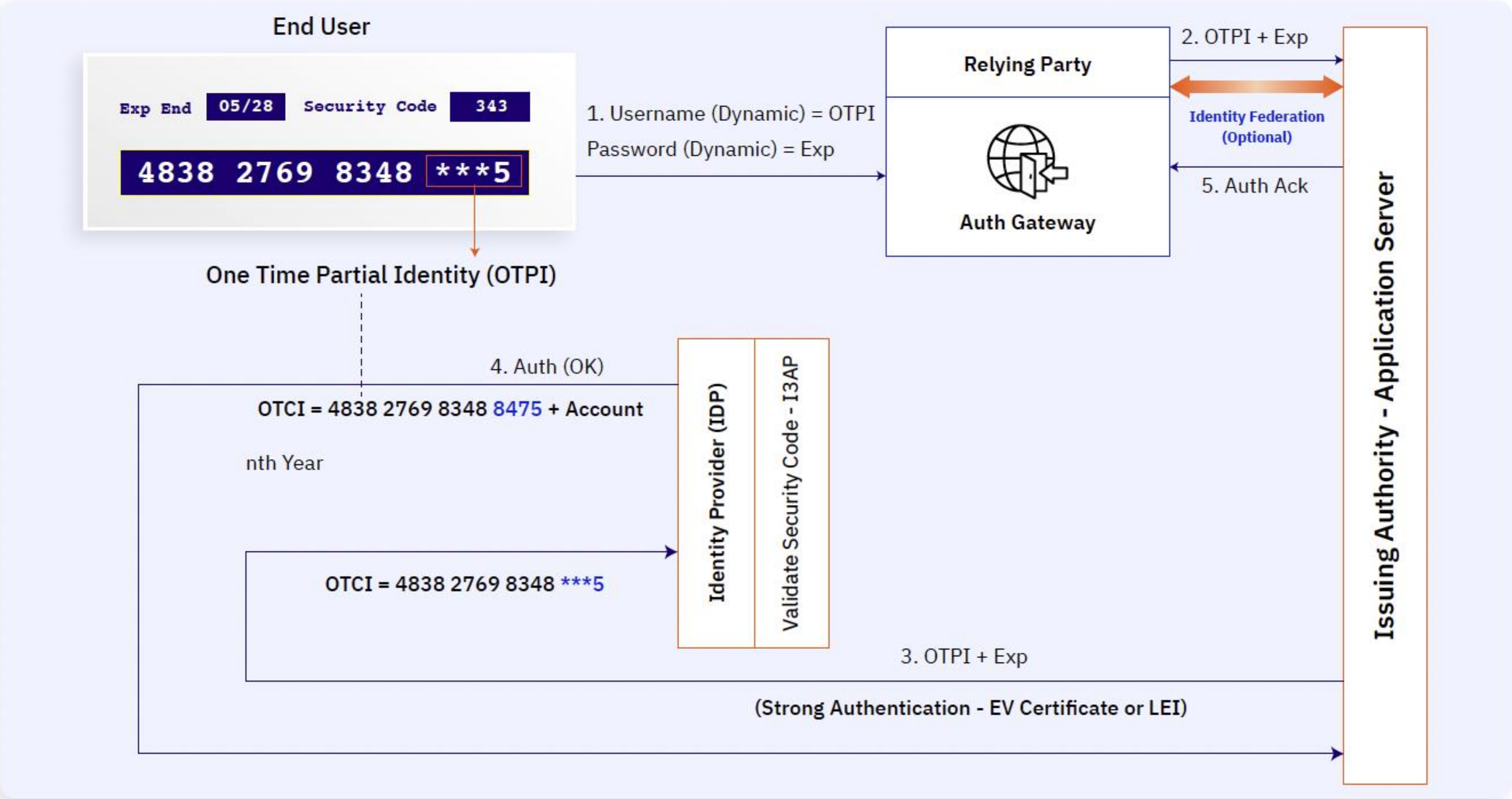
Identity Provider (IDP)

Validate Security Code - I3AP

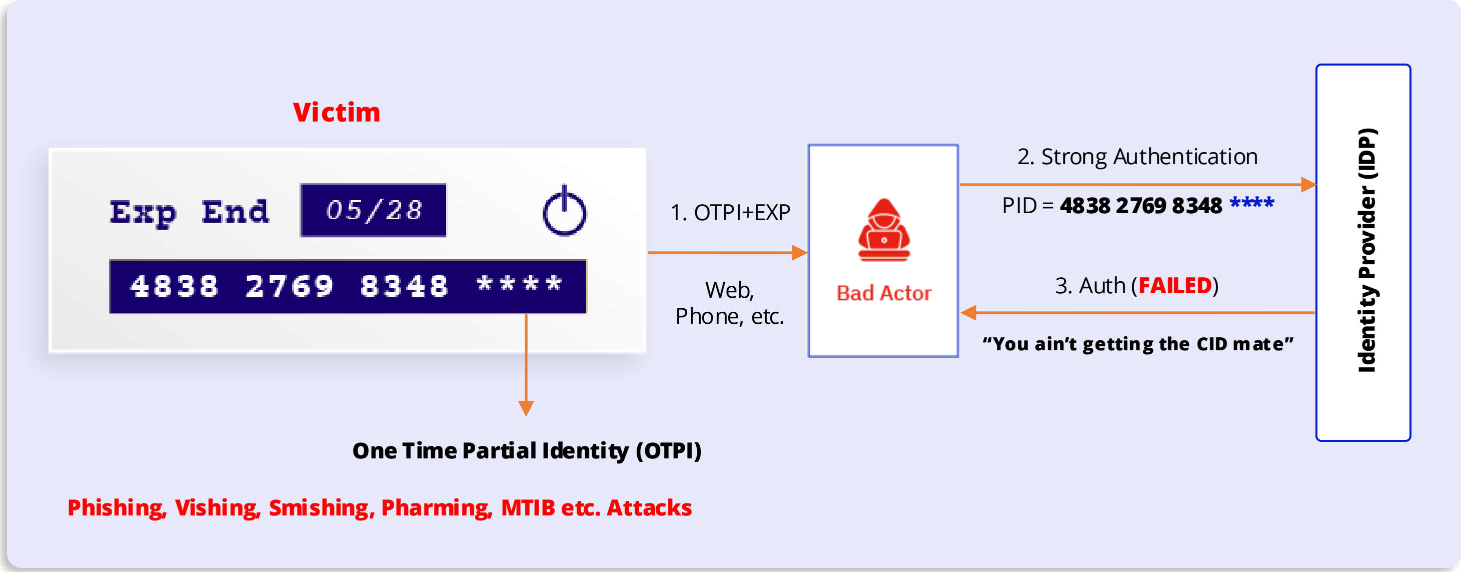
3. OTPI + Exp

(Strong Authentication - EV Certificate or LEI)

Online Authentication – Identity Federation


End User
Exp End
05/28
Security Code
343
4838 2769 8348 ***5
One Time Partial Identity (OTPI)
1. Username (Dynamic) = OTPI
Password (Dynamic) = Exp
Relying Party
Auth Gateway
2. OTPI + Exp
Identity Federation (Optional)
5. Auth Ack
Issuing Authority - Application Server
4. Auth (OK)
OTCI = 4838 2769 8348 8475 + Account
nth Year
OTCI = 4838 2769 8348 ***5
Identity Provider (IDP)
Validate Security Code - I3AP
3. OTPI + Exp
(Strong Authentication - EV Certificate or LEI)

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

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 ID

1. The technique offers **Dynamic Personally Identifiable Information (DPII).**

2. DPII **defends against all known identity attacks such as** Identity skimming fraud, phishing, 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 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. 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 ID,, Bank Card numbers etc. & b) the expiration date of the identity. This greatly **addresses privacy concerns**.

5. 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**.

6. This concept is broad-spectrum & can secure both **physical** & **online** identities.

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

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

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

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.

Thank You

10S Technologies