10S Technologies

Ānśik ID

Online Authentication

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 skimming & social engineering fraud.

b) Phishing, vishing & smishing.

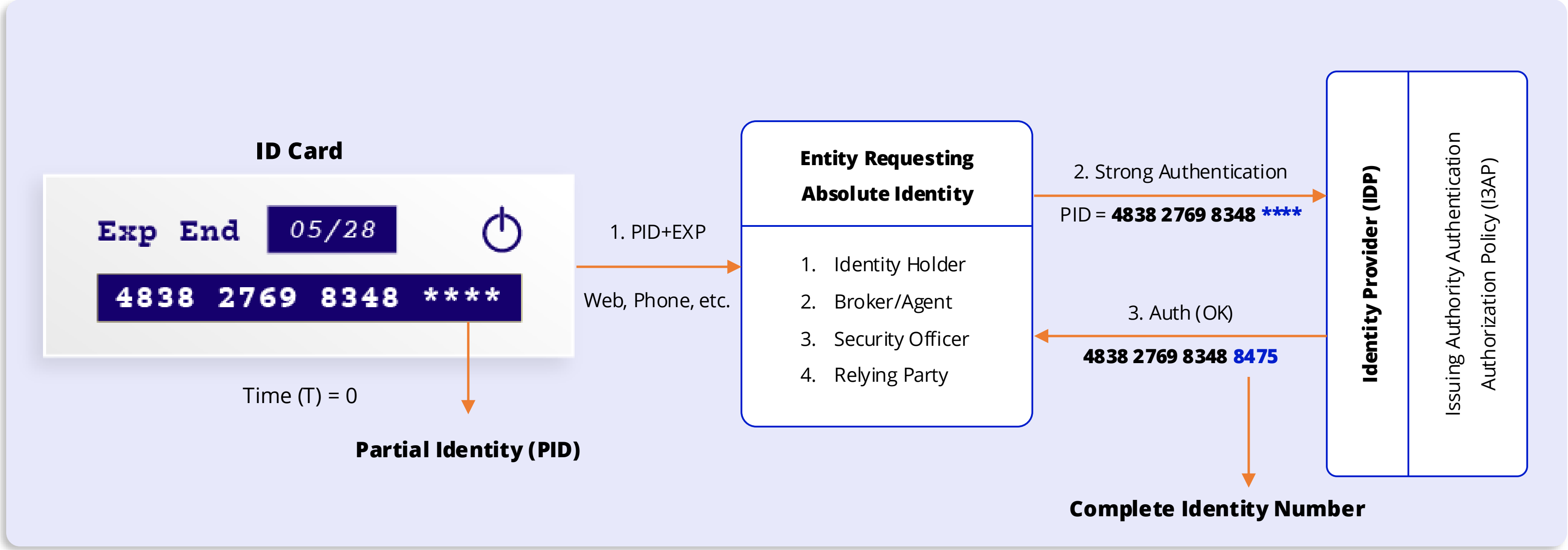
c) Pharming & Man-In-The-Middle (MITM).

d) Insider fraud & Database breach etc.

Various online identities can be protected for example 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 corporates, service provider applications etc.

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)

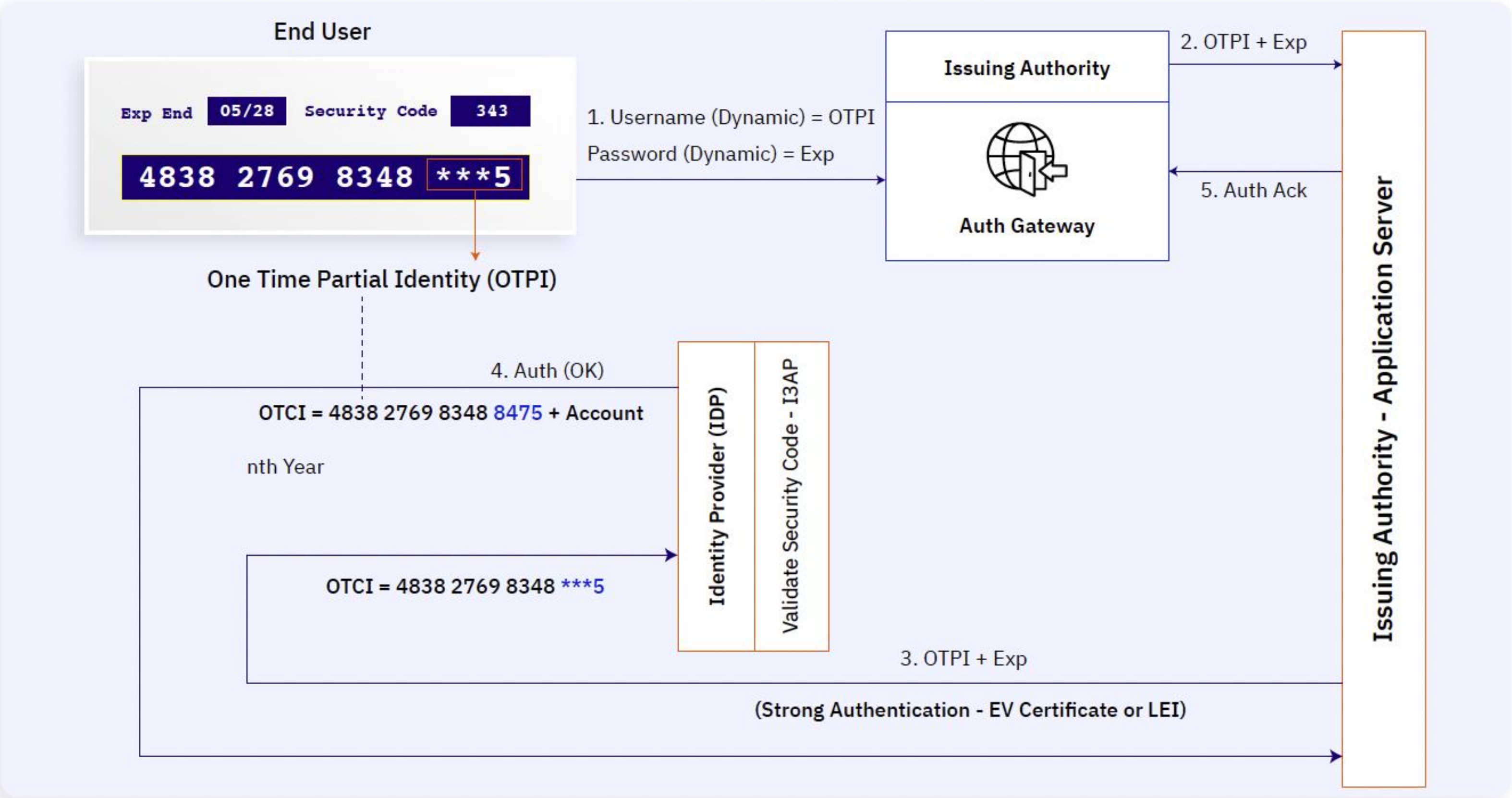
T=0 min, PID = 4838 2769 8348 * & OTCI returned = 4838 2769 8348 8475***

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.

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

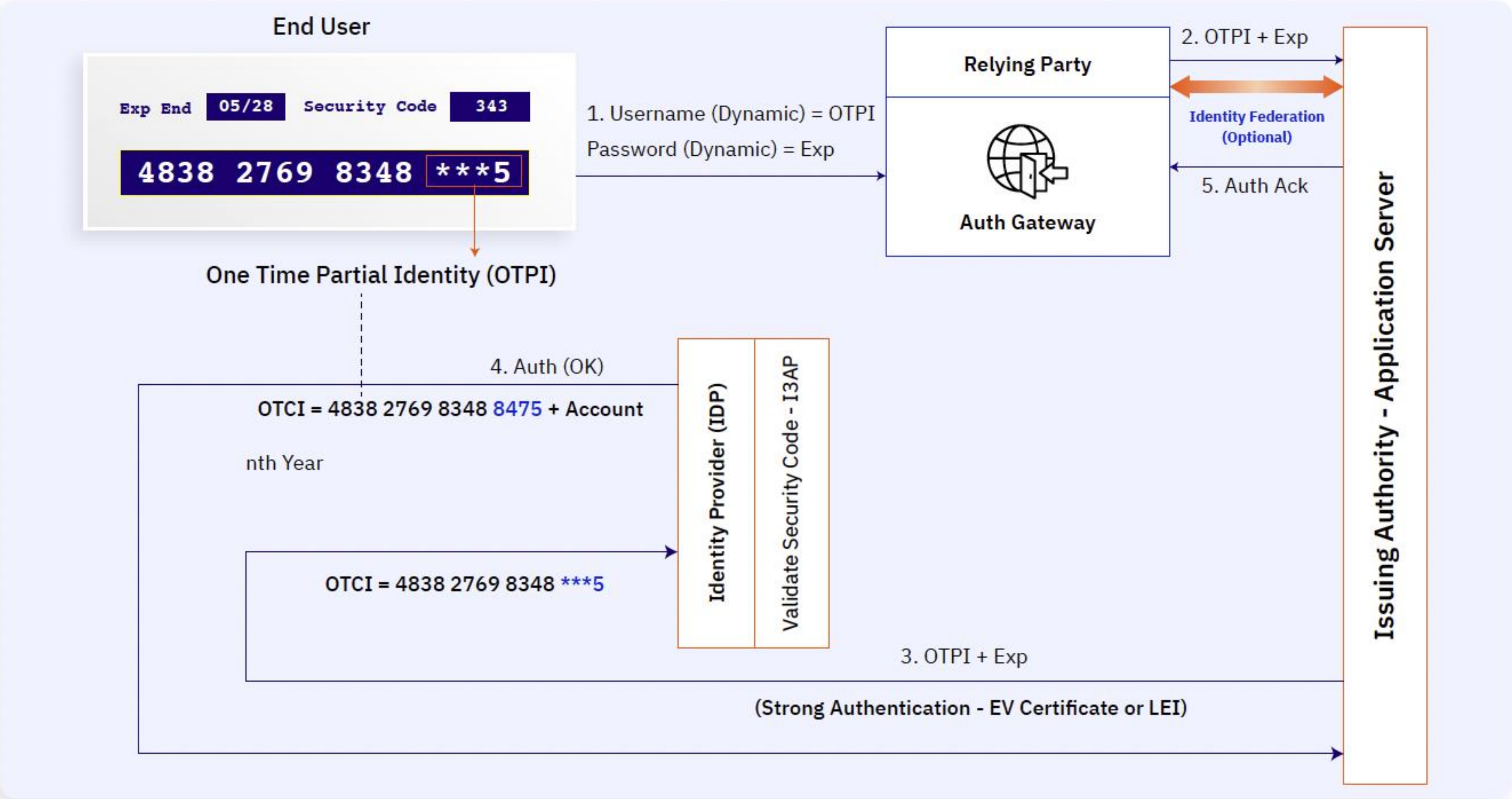

End User
Exp End 05/28 Security Code 343
4838 2769 8348 ***5
One Time Partial Identity (OTPI)
1. Username (Dynamic) = OTPI
Password (Dynamic) = Exp
Issuing Authority
Auth Gateway
2. OTPI + Exp
5. Auth Ack
Issuing Authority - Application Server
4. Auth (OK)
OTCI = 4838 2769 8348 8475 + Account
nth Year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

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

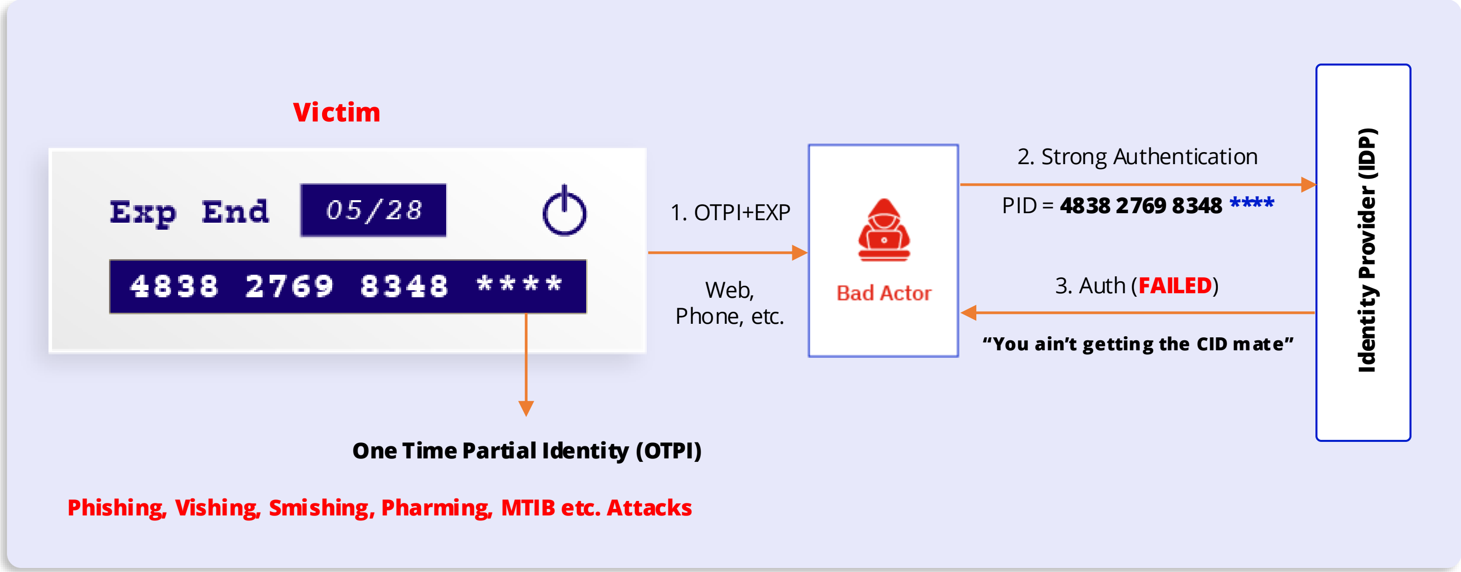
b) OTPI produces 'dynamic usernames' or One Time User Name (OTUN). We can completely eliminate username as an attack vector.

c) Expiry date can serve as a dynamic password.

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

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, and MFA vulnerabilities.

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

4. 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**.

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

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

Thank You

10S Technologies

© 2025 All rights reserved