10S Technologies

GOVERNMENT ID DATASHEET

Dynamic Partial ID

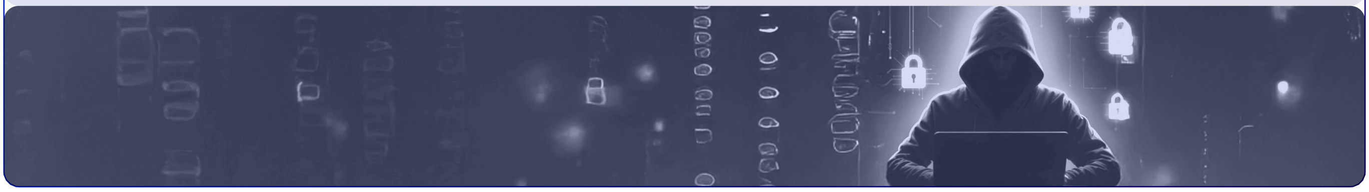
ABSTRACT/FIELD OF INVENTION

Globally, identity fraud costs people, businesses, and governments more than USD 1 trillion each year! This patent pending invention relates to safeguarding personally identifiable information (PII) from various forms of attacks on 'online' and 'real world/physical' identities. Name, expiration date and other details on physical IDs like passports, national identification cards, bank cards, etc. are examples of PII. The technique also provides PII security for online identities, such as username/passwords. All known identity threats such as skimming, phishing, pharming, photocopy fraud etc. will be prevented by this technique. Both hardware and software identity smart cards will be offered to support the technique.

BACKGROUND

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 million 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.**



Measuring the worth of “trust” is one more technique to evaluate the effects of identity fraud. Additionally, trust can be institutionalised or formalised. As a result, more people can conduct business with one another. The only way to increase wealth for people, organisations, and the economy as a whole is to conduct more commerce. According to Steve Knack, a senior economist at the World Bank who has been researching the “Economics of Trust” for more than ten years, trust is worth 99.5% of a country’s economy or GDP!

An examination of multiple fraudulent situations reveals a basic weakness in every identity on the planet - the private information about an individual is immutable and is printed on the ID card for an extended period of time - this is true for online identities - the username remains static. Once compromised, the information can be sold on the Dark Web or used improperly to initiate other types of assaults.

The novelty offered by this technique is **Dynamic Partial ID** which completely eliminates static PII & cannot be compromised by means of phishing, vishing, smishing, pharming, Man-In-The-Middle (MITM), ID card skimming, photo copy fraud, insider fraud, shoulder surfing and others.

The ID 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’. Issuing Authorities define several parameters for example expiry of the identity. Examples of Issuing Authorities are Government bodies issuing passports, Driving licenses, National Identities, voter IDs or even banks etc.

DESCRIPTION

Figure 1

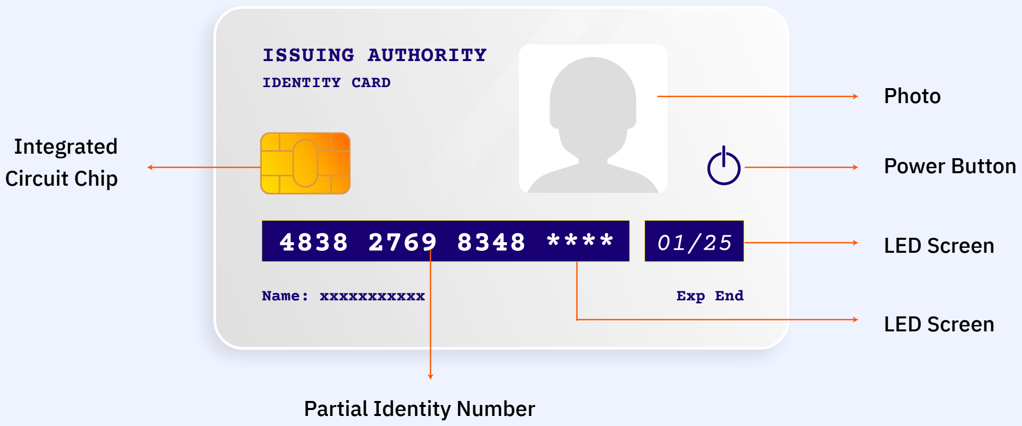
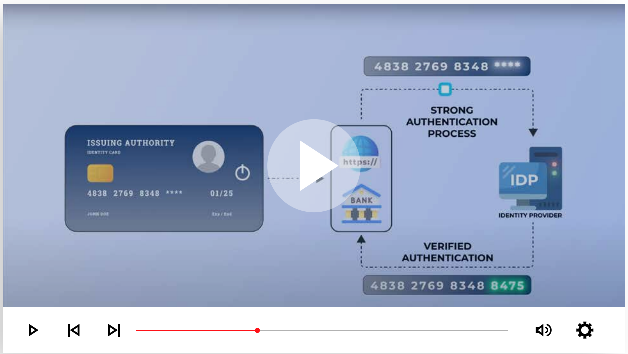


Figure 1: This figure describes the components of proposed identity card.

Identity Number: The ID card number or Primary Account Number (PAN) will renew as often as the issuing authority and its security posture will determine. As an example, we shall maintain this ‘time interval’ at five minutes. Stated differently, the card number will be reset every five minutes.

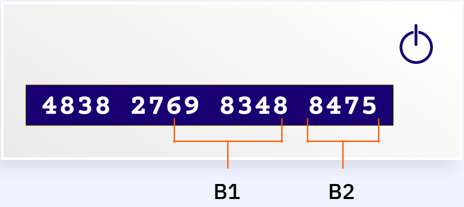
ID Expiry: Depending on the security posture of the issuing authority, an expiration date can be defined for each new identity number shown. In other words, every identity displayed will be valid for ‘n’ months in the Identity Provider (IDP) system. When the power button is pressed, both of these values are shown on LED screen. The power button may also be configured with biometrics to provide an extra layer of authentication. When an ID is issued, biometric finger prints will be used for deduplication purposes.

One of the system's innovations and a key distinction is that the ID card won't show the entire identity number. Rather, a Partial Identity Number (PID) is displayed, for example 4838 2769 8348 ****. In this example, the final four numbers are shown on the screen as '*'.



Youtube Video

Figure 2



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

B2 = Logical Block 2 (Changes every 5 minutes)
SS2 = Shared Secret 2

Figure 2: The identity number on the suggested ID card will be divided into two or more logical parts. In this example, we consider two blocks B1=698348 and B2=8475. The time intervals, as an example, are B1 (1 year), B2 (5 minutes). The number of bits might, however, differ with different implementations. A shared secret (SS) key corresponds to each of the logical blocks. In this example, B1 corresponds to SS1 and B2 with SS2. In a FIPS-certified end-user smart card, these shared keys are stored securely and are not exportable. These symmetric keys, for example, could be Advanced Encryption Standards (AES) keys

The identical shared secrets will likewise be mapped to specific user account in the IDP system and kept encrypted in database supported by FIPS certified Hardware Security Modules.

PID is all that the malicious actor will learn in a Man-in-the-Middle attack because the ID card does not display the full Identity Number. One possible attack vector for determining the full identity number is a brute force attack. The likelihood of accurately guessing a three-digit number in a single try, where each digit can be any number from 0 to 9, is 0.1%. Thus, in comparison to statically printed Identity number, the proposed technique is 99.9% secure!

For illustration, the obfuscated digits (shown as **** on LED) are actually 8475. Steps to generate this value by the smart card and IDP is described in detail in the **Whitepaper (page #8)**.

In order to complete end user authentication, the B2 value is computed at IDP, which also has similar time intervals as the ID card.

Figure 3

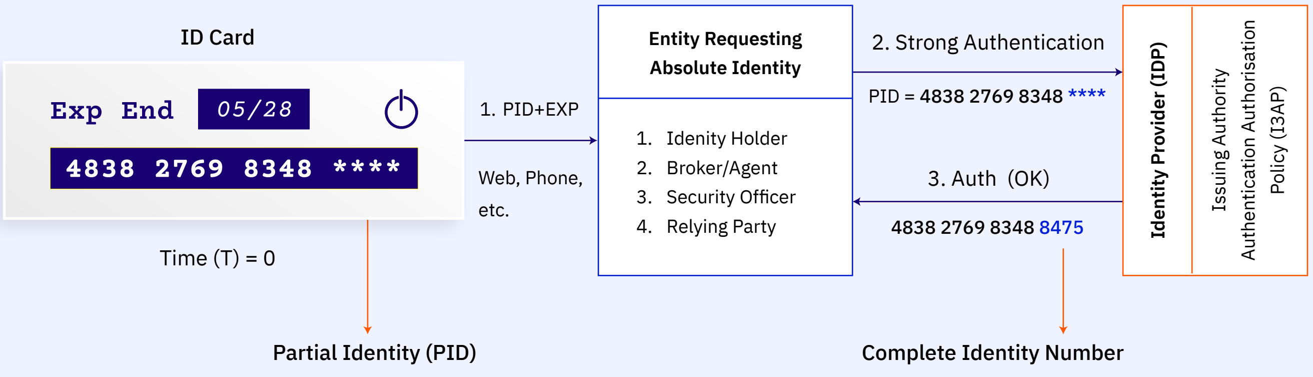


Figure 3: In this embodiment, the Partial Identity (PID) and Expiry will be shown on the Identity smart card with a single button push. The concerned entity will then need to get in touch with the Identity Provider (IDP) in order to obtain the full Identity. It is important to remember that the Identity number changes after a predetermined threshold time interval, for example, five minutes. The authentication flow is as follows:

*1) At T=0 minutes, the user pushes the Identity smart card button and PID (4838 2769 8348 ****) and Expiry date are displayed. PID and date of expiration are sent to relying party.*

2) In order to obtain the Full ID, relying party (RP) must authenticate with the Identity Provider (IDP). PID and date of expiration are sent to IDP.

3) If RP authentication passes, IDP will verify the incoming expiration date and compute B2 in order to deduce the absolute ID. Because it has SS2, IDP will carry out a procedure akin to that carried out by the smart card and obtain B2. When B2 is appended to the PID, complete identity is ready for shipping. The complete ID (4838 2769 8348 8475), which is essentially the identity number, is returned by the IDP. This ID number is required by the RP to finish the end user transaction.

At T= 5 minutes (after 5 minutes), the end user Smart Card displays PID=4838 2769 8348 **** and identity returned by IDP is 4838 2769 8348 0076.

NOTE THE FOLLOWING

1. First 12 digits of PID and Identity Number returned are same as before.
2. The identity returned by IDP has changed in a pre-configured time interval of five minutes. Because the identity number returned only appears once, it goes by the name **One Time Complete Identity (OTCI).**
3. An Identity holder can have multiple unique OTCI associated at any given point in time and each OTCI will have its expiry decided by the Issuing Authority.
4. These unique OTCIs are tied to respective Relying Parties who consume these identities.

An Issuing Authority, for example Department of transport issuing Driving License, can retain the returned Complete ID in a static state for an extended period of time, say five or ten years. This is referred to as **Complete ID (CID)**. One of the significant advantages of this strategy is that CID can be cached on service provider websites (for KYC) or mobile apps as it is currently done. Thus, convenient for the end-users. Having stated that, the drawback of CID is that it is prone to replay attack, fraudulent administrator attacks or database breach.

It is significant to remember that all communication occurs over mutual Transport Layer Security (mTLS), which encrypts data while it is in transit.

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

1) NATURAL PERSON

For phone or broker initiated transactions, the system will support smart card based authentication, which can be standard RFID/NFC identities such as ePassports, National IDs etc. or potentially the ID card itself can be used towards this purpose. All-Natural Person relying party will have a) NFC smart card, b) device to fetch CID and c) their smart cards linked to a App. I3AP (below) will allow the Natural Person to cache their identity information for certain period of time. In subsequent phases, the proposed system will offer a smart card with Natural Person Identity (NP ID) authorization. An example could be Public Key Infrastructure (PKI) based asymmetric keys and digital certificates securely stored in FIPS-certified chip. PKI offers a significant advantage of leveraging digital signatures to achieve non-repudiation and legal tangibility

2) MACHINE-TO-MACHINE (M2M)

Online transactions will leverage Legal Entity Identifier (LEI) or Organization Validated (OV) public certificates.

Issuing Authority Authentication Authorization Policies (I3AP) can **a)** prohibit any natural person from obtaining the OTCI; instead, the relying party/application accepts the PID, authenticates to IDP, retrieves the OTCI, and completes the transaction, **b)** allow Identity Holder Consent for OTCI/CID fetch by RPs, **c)** contact based or contactless transaction, **d)** PIN or biometric based Mobile App Authentication mode, **e)** PID and Expiry Date Synchronization, **f)** time interval after which the identity number (OTCI) will change & **g)** allowed incorrect PID attempts.

All I3AP policies are described in detail in the **Whitepaper (page #12)**.

If the issuing authority expects a range of user scenarios, hardcoding the identity validity at the time of issuance will be challenging. One approach to addressing this might be to provide the relying party with dynamic expiration dates along with CID! This method eliminates the need for an expiration date LED on the ID card.

An extension of the this concept and intriguing embodiment may be smart cards with no LEDs at all! The end user uses NFC to tap the ID card on their mobile phone, and IDP pushes the OTCI and expiration dates to the mobile app. This approach will help lower the cost of ID cards.

Cards that are solely software-based could be another economically viable solution. The shared secrets of the end user are stored and secured on their mobile device. The user will use the smartphone app in place of a real NFC tap.

Another embodiment can be Smart Card enabled with a SIM or eSIM card so that, in accordance with I3AP policies, the OTCI/CID and/or expiration date can be pushed straight to the ID card and shown on the LED screen at the touch of a button. For pros and cons of software and eSIM enabled cards, refer the Whitepaper.

ONE-TIME PARTIAL IDENTITY (OTPI)

This 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.

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

T=5 min, PID = 5849 3979 6061 201 ** 4 & OTCI returned = 5849 3979 6061 278 37 4

T=10 min, PID = 5849 3979 6061 203 ** 4 & OTCI returned = 5849 3979 6061 278 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.

Figure 4

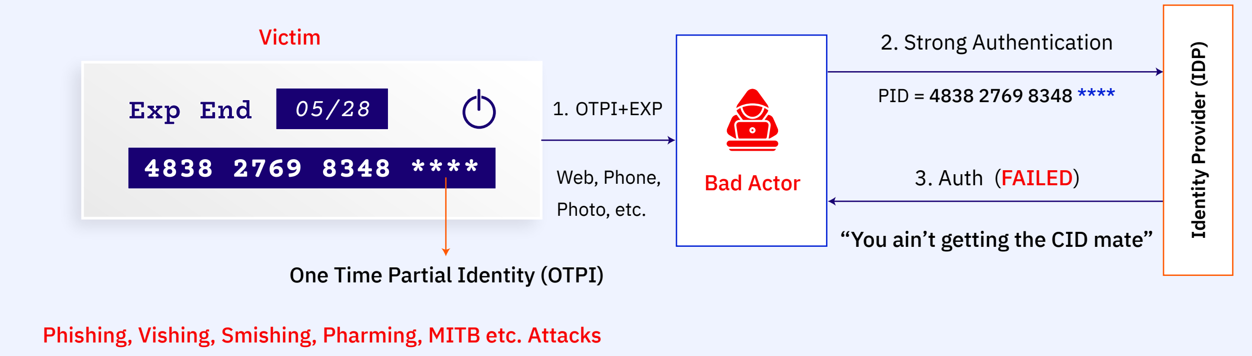

Victim
Exp End
05/28
4838 2769 8348 ****
One Time Partial Identity (OTPI)
1. OTPI+EXP
Web, Phone, Photo, etc.
Bad Actor
2. Strong Authentication
PID = 4838 2769 8348 ****
3. Auth (FAILED)
"You ain't getting the CID mate"
Identity Provider (IDP)
Phishing, Vishing, Smishing, Pharming, MITB etc. Attacks

Figure 4 Now let's look at how this system and method will aid in thwarting several identity card-related threats. The process below illustrates a fraudster targeting a victim and attempting to steal identity information for example Driving License number, expiration date etc. This assault can be initiated by any medium for example SMS, email, web, phones etc.

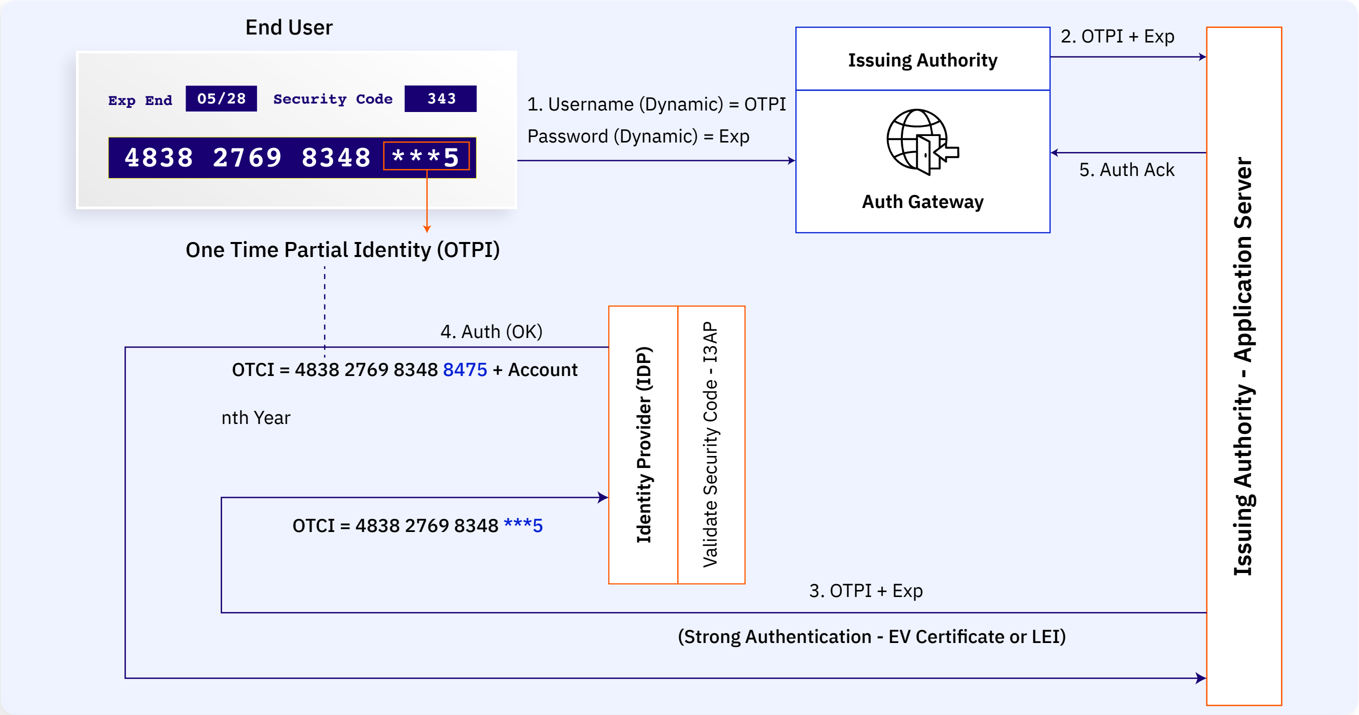
- *The unsuspecting victim ends up giving the attacker the Partial Identity Number and expiration date.*
- *The scammer requires the Complete identity in order to use the identity fraudulently. With traditional ID cards, it would be game over by now. Since the complete card number is not displayed by this technique, the adversary contacts IDP and needs to authenticate.*
- *This verification puts up a barrier. Because the fraudster wouldn't have the necessary credentials and authorization, hence their attempt to steal identity data would be fruitless.*

The Complete ID or 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 fraud is reported thus guaranteeing that future fraud is avoided by same fraudster.

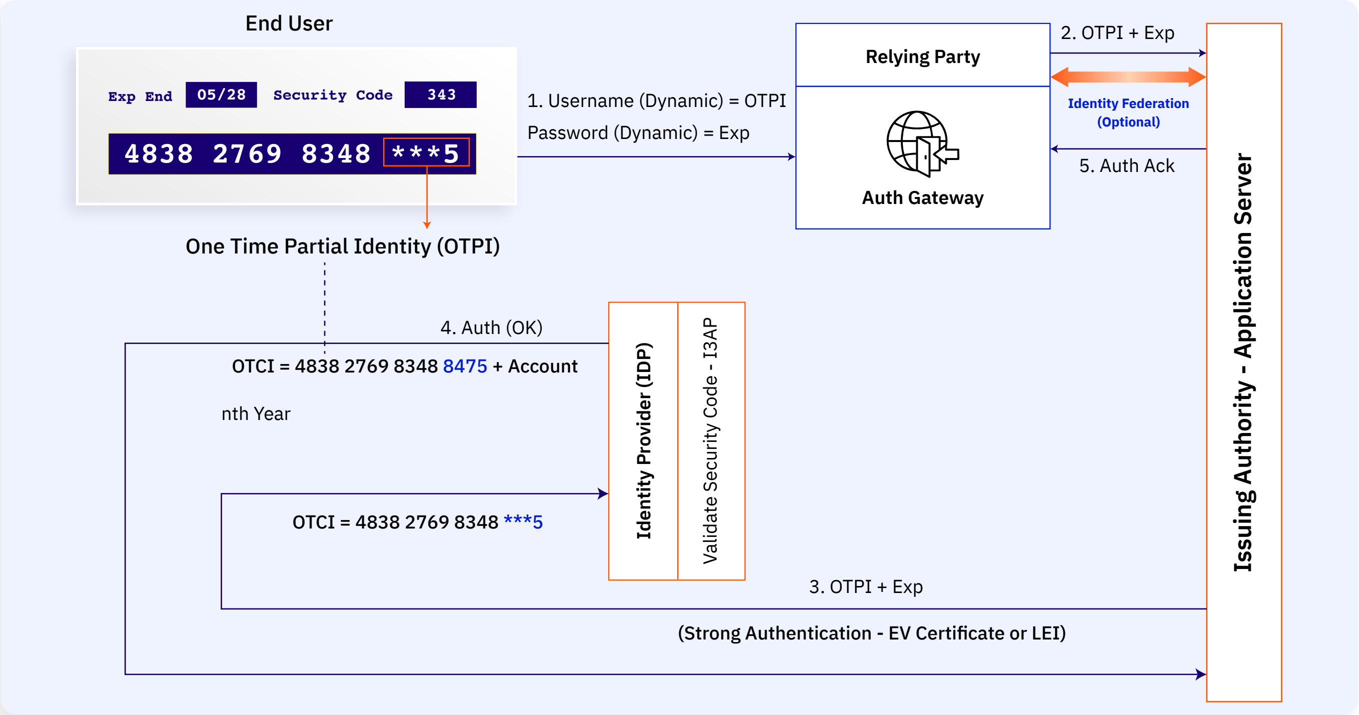
Even though identity number is dynamic, it is mapped to the static user account number printed on the smart card. The detailed process is described in the **Whitepaper (page #17)**.

The technique can be used to secure online identities as well. The following mechanisms are available for use a) The PID displayed on the card interface can act as username, b) Usernames are almost always static for online accounts and is an attack vector! Dynamic OTPI may be used to produce "dynamic usernames," an additional security layer that will deter fraudsters. This can be termed as One Time User Name (OTUN) & c) the card Expiry date can serve as a dynamic password.

Online 2FA Use case


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
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)
Issuing Authority - Application Server

The proposed method and system can be leveraged for online authentication well. The novelty offered by the system is dynamic username – we eliminate static username as an attack vector. OTPI serves as dynamic username. The Expiry date serves as dynamic password, which can be configured to change every 5 min.


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
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)
Issuing Authority - Application Server

The system will support Identity federation as well. Hence Identity issued by one organization (Issuing Authority), can be leveraged by others (Relying party) effectively.

Advantages of Dynamic Partial ID

1. The technique offers **Dynamic Personally Identifiable Information (DPII)**.
2. This concept is broad-spectrum in nature and can secure both physical and online identities.
3. In order to accommodate different needs & the security posture of the issuing authority, 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 I3A policies are available and can be configured in real-time.
5. OTPI and PID can successfully assist in defending against card skimming fraud, phishing, vishing, smising, MITB, pharming, insider fraud and other forms of attacks that target PII.
6. Banks will significantly reduce logistical costs since there will be no need to reissue and ship cards because of their expiration.
7. 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.
8. There is no need for end-user education or awareness campaigns warning users not to share card data or other 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 (banks) can be used by other relying parties (Government departments, corporates etc.) This can be an additional source of revenue for issuing authorities!

IDENTITY THREATS AND MITIGATION MATRIX

Threat	Description	Mitigation
Card Skimming	A fraudster gets victims' ID card details via skimming devices, hidden cameras followed by data extraction and card cloning. This is data is misused later.	1. The ID Card only displays partial ID & to fetch Complete ID/OTCI, all relying parties must authenticate with the IDP. 2. OTCI is mapped to unique RP. 3. OTCI expiry can be dynamic and short lived.
Man-in-the-Middle	The attacker intercepts the credentials and data while they are in transit. In this case, the attacker appears as the relying party to the user and as the user to the target server.	1. The card only displays partial ID & to fetch OTCI, all relying parties need to authenticate with the IDP. 2. All data in transit is encrypted via mTLS. 3. End user Mobile Push Notification approval provides an additional layer.
Phishing, Vishing, Smishing	The attacker targets unsophisticated and unsuspecting victims and tricks them into sharing their ID card details.	The ID Card only displays partial ID & to fetch OTCI, all relying parties must authenticate with the IDP.
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.	The ID card only displays partial ID & to fetch OTCI, the pharming site must authenticate with the IDP and that's when it fails. Our model proposes organization level vetted identifiers such as OV public certificates or LEI.
Replay attack	This attack follows from ID card skimming, MITM, phishing, pharming, inside fraud or DB breach. Compromised data is misused (or replayed) at a later time to perpetrate identity theft.	1. OTCI expiry can be dynamic & adjusted based on risk assessment. If relying party's Data Protection Regulation is not assured or OTCI cannot be binded to relying party, OTCI expiry is kept short. 2. Relying Party ID is mapped to OTCI to establish accountability.

Threat	Description	Mitigation
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.	Since the ID card only displays partial ID, all the key logger will get is incomplete information. To fetch Complete ID, it must authenticate with the IDP and that's when it fails.
Malware Browser Memory Attack	The attacker attempts to find the credentials downloaded in the memory of a system.	Shared Secret (Symmetric) keys will be stored in FIPS/CC certified hardware smart card hence completely eliminates this attack.
Brute Force	Attacker exhaustively attempts all possible combination of missing identity data in PID or OTPI, which eventually leads to guessing the correct one, thus giving them OTCI.	1. With OTPI and PID, the system is between 99.7% & 99.99% secure to brute force attacks. 2. I3AP Policy can limit the number of OTPI/PID attempts before blocking the account.
Fraudulent Admin or database breach.	A fraudulent administrator gets access to PII on the server and misuses it. It is true in case of a database breach as well.	1. OTPI ensures data cannot be cached. 2. OTCI is mapped to unique RP & as such, this is the only RP which can consume it again.
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.	This method causes cards to display only partial IDs. In order to obtain the OTCI, an entity must first authenticate with the IDP. That is where the fraudster will be caught.
Photocopy Fraud	When a victim needs to avail a specific service, they give a photocopy of their identity card. A dishonest employee misuses this information.	Only partial IDs are shown on smart card using this strategy. Any entity that is eager to fetch the OTCI will need to authenticate with IDP.
Multi factor Authentication vulnerability	Absolutely all authentication attacks commence from identifying victims' username, which is always static.	With OTPI as dynamic username, changing frequently, we completely eliminate this attack vector. Additionally, the technique can provide dynamic passwords too.

THREAT MITIGATION COMPETITIVE ANALYSIS - DYNAMIC PARTIAL ID VS GOVERNMENT ID

TYPE ID		GOVERNMENT ID		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
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
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	YES	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
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
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 ?	NO	YES	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.	<NO>	<NO>	YES	YES
MFA Vulnerability	Does the ID card/system itself enhance online access 2FA?	NO	NO	YES	YES
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?	NO	NO	YES	YES
	TOTAL SCORE	5/17	6/17	17/17	15/17
	PERCENTAGE	30%	35%	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

Renewable Identity technique constitutes a crucial competent 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.