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.