

Feasibility of a biometric-based digital identity app replacing physical ID cards

Table of Contents

1. Executive Summary
 2. Introduction
 3. The Concept of Biometric-Based Digital Identity
 4. Technical Foundations and Requirements
 5. Legal and Regulatory Landscape in Canada
 6. Legal and Regulatory Landscape in the United States
 7. Comparative Analysis of Privacy Frameworks
 8. Barriers for Vulnerable and Homeless Populations
 9. Security Risks and Biometric Template Protection
 10. Self-Sovereign Identity as an Alternative Paradigm
 11. Feasibility Analysis for a Vancouver Pilot Project
 12. Pathways for North American Expansion
 13. Proposed Framework and Recommendations
 14. Conclusion
-

1. Executive Summary

The rapid proliferation of digital technologies has created new opportunities for identity verification through biometric authentication on mobile devices. This report examines the feasibility of developing a standardized biometric-based digital identity application that could replace physical identification cards, using the BC Services Card mobile application as a reference point. The proposed system would enable user authentication via on-device biometrics, provide no-cost replacement of digital credentials, and minimize data sharing with third parties. The analysis incorporates privacy legislation in Canada and the United States, examines barriers to adoption including access for homeless populations, and evaluates technical requirements derived from the National Institute of Standards and Technology Digital Identity Guidelines. Our findings indicate that while the technical building blocks exist to create such a system, significant hurdles remain due to fragmented

regulatory frameworks, biometric security vulnerabilities, and infrastructure requirements that may exclude vulnerable populations. A pilot project in Vancouver is feasible with appropriate privacy-by-design principles and self-sovereign identity architecture, but expansion across North America would require harmonization of varying state-level biometric privacy laws and substantial investment in accessible technology infrastructure.

2. Introduction

Biometric identification, defined as the use of unique physical or behavioral characteristics to identify individuals, has been a feature of security systems for decades. Advancements in technology have greatly expanded the types of biometric information that can be collected and the ways such information can be used. Facial structure, fingerprints, speech patterns, voice recognition, iris composition, retinal scans, gait, hand geometry, vein patterns, and even body odor are examples of biometric identifiers ⁸. The purposes for which biometric data may be used fall into four categories: permitting physical access to restricted areas, confirming an entitlement to services, monitoring or recording certain facts, and associating a particular activity with an individual ⁸.

The British Columbia Services Card mobile application represents a notable step toward digital identity verification. This application allows residents to access government services through their mobile devices, but it does not yet function as a full replacement for physical identification across all sectors. The concept of a comprehensive biometric-based digital identity application that could serve banking, voting, and other critical functions raises important questions about technical feasibility, legal compliance, and social inclusion.

The growing reliance on biometric and geolocation technologies has prompted lawmakers to shift focus from traditional data protection toward more stringent regulations governing biometric data collection and use ³. As of 2017, three states have enacted biometric privacy laws, and five additional states have introduced bills governing biometric data ³. This regulatory evolution reflects the recognition that biometric data, unlike passwords or numerical identifiers, cannot be replaced or modified if compromised. Victims of identity theft can change their account numbers or taxpayer identification numbers, but facial geometry and fingerprints cannot be replaced ³.

3. The Concept of Biometric-Based Digital Identity

A digital identity is a digital representation of a person's identity, as opposed to physical identity cards that individuals carry ³. The National Institute of Standards and Technology defines digital identity as "the unique representation of a subject engaged in an online

transaction" 4 . Digital identity is always unique in the context of a digital service but does not necessarily need to be traceable back to a specific real-life subject 4 .

The proposed mobile application would operate on the premise that biometric authentication, combined with secure storage on the device itself, could replace the need for physical identification cards. The system would store biometric templates locally on the user's smartphone rather than on a central server. This approach aligns with the concept of "untraceable biometrics" described by the Ontario Privacy Commissioner, which enables processing and use of biometric information without associating it to an identifiable individual because it does not store biometric images or templates from which the original data could be recreated 8 .

The authentication process would involve the user presenting their biometric characteristic to the device's sensor. The biometric data submitted by the individual would be irreversibly and untraceably converted into an unrelated data string, personal identification number, or key. When the individual re-presents the biometric information, the unique PIN or key is recreated and compared with the stored string. This approach employs a "one-to-one" verification rather than "one-to-many" identification, meaning the information about one individual is stored and compared with a live sample provided by that same individual 8 .

Key Features of the Proposed System:

Feature	Description	Implementation Approach
On-Device Storage	Biometric templates stored locally on smartphone	No central biometric database; templates encrypted and stored in device secure enclave
No-Cost Replacement	Digital credentials re-issuable without physical card production	Verifiable credentials stored on device; can be restored from secure backup or re-issued by trusted authority
Minimal Data Sharing	Only essential attributes shared with verifiers	Zero-knowledge proofs and selective disclosure of claims
Multi-Purpose Authentication	Replaces physical ID for banking, voting, and other services	Standardized attestation framework with verifiable credentials

Feature	Description	Implementation Approach
Biometric Authentication	Fingerprint, face, or iris scan for verification	On-device biometric matching; biometric used as second factor with PIN as primary

4. Technical Foundations and Requirements

The technical implementation of a biometric-based digital identity application must satisfy the requirements established by the National Institute of Standards and Technology Digital Identity Guidelines (SP 800-63B). These guidelines define three Authenticator Assurance Levels (AALs) that determine the strength of authentication required for different applications.

4.1 Authenticator Assurance Levels

At AAL1, single-factor authentication is acceptable, and communication between the claimant and verifier must occur via an authenticated protected channel 4 . Reauthentication should be performed at least once per 30 days during extended usage sessions 4 .

AAL2 requires multi-factor authentication using two different authentication factors. When a biometric factor is used at AAL2, performance requirements must be met, and the verifier should determine that the biometric sensor and subsequent processing meet these requirements 4 . Reauthentication must be performed at least once per 12 hours during extended usage sessions and following any period of inactivity lasting 30 minutes or longer 4 .

AAL3 provides the highest level of assurance. The verifier must make a determination that the biometric sensor and subsequent processing meet the performance requirements 4 . Reauthentication at AAL3 must use both authentication factors and must occur after 15 minutes of inactivity 4 .

4.2 Biometric Authentication Requirements

The NIST guidelines specify that biometrics should be used only as part of multi-factor authentication with a physical authenticator (something you have) 4 . The biometric system must operate with a False Match Rate of 1 in 1000 or better, achieved under conditions of a zero-effort impostor attempt 4 .

The system must limit consecutive failed authentication attempts to no more than five, or ten if Presentation Attack Detection meeting requirements is implemented. Once this limit is reached, the biometric authenticator must either impose a delay of at least 30 seconds before the next attempt (increasing exponentially with each successive attempt) or disable biometric user authentication and offer another factor ⁴ .

NIST supports only limited use of biometrics for authentication for several reasons. The biometric False Match Rate does not provide confidence in authentication by itself and does not account for spoofing attacks. Biometric comparison is probabilistic while other authentication factors are deterministic. Biometric characteristics do not constitute secrets because they can be obtained online or by taking a picture, lifted from objects someone touches, or captured with high-resolution images ⁴ .

4.3 On-Device vs. Off-Device Comparison

The Personal Identity Verification standard allows for both off-card and on-card comparison of biometric data. Off-card comparison involves storing templates on the card and comparing them with templates collected during authentication on a reader device. The cardholder must enter a PIN to release the templates, and when the card is cryptographically authenticated, this constitutes multi-factor authentication ⁵ .

On-card comparison offers an alternative to PIN-mediated card activation. The main attraction of on-card comparison is that someone who finds a card has only a small chance of authenticating with fingerprints because the template data never leaves the card ⁵ . In the off-card comparison world, PIN entry is used to mitigate this risk ⁵ .

For the proposed mobile application, on-device comparison would be the preferred approach. The biometric template would remain stored within the device's secure enclave, never transmitted to external servers. This approach provides greater privacy protection and reduces the risk of large-scale biometric data breaches.

5. Legal and Regulatory Landscape in Canada

Canada's approach to biometric data privacy is governed primarily by the Personal Information Protection and Electronic Documents Act (PIPEDA) at the federal level. British Columbia, Alberta, and Quebec each have their own private sector privacy legislation regulating the flow of personal information within provincial borders ⁸ .

5.1 PIPEDA Requirements

PIPEDA regulates the collection, use, and disclosure of personal information in the private sector for all commercial activities involving cross-border flows of personal information ⁸ . The legislation is based on fair information handling practices, which include informed consent, reasoned and limited collection, use and disclosure of personal information, and ensuring such personal information is adequately secured ⁸ .

The application of PIPEDA to biometric data involves a four-part test that evaluates the appropriateness of the purpose for collecting personal information. This test asks: (1) is the measure demonstrably necessary to meet a specific need; (2) is it likely to be effective in meeting that need; (3) is the loss of privacy proportional to the benefit gained; and (4) is there a less privacy-invasive way of achieving the same end ⁸ .

The Office of the Privacy Commissioner of Canada has issued comprehensive guidance on processing biometrics under PIPEDA, emphasizing a higher bar for compliance. The guidance clarifies that biometric data, including facial geometry, is considered sensitive by default, necessitating stringent requirements for consent, safeguards, and reporting ² . Express consent is the default requirement for biometric data processing, meaning consent must be explicit, informed, specific to biometrics, integrated into user flows, and renewable. Organizations must also provide opt-out options and alternatives, especially when biometrics are not essential to their product or service ² .

5.2 Four-Part Test for Biometric Deployment

Before deploying biometric technology, PIPEDA requires demonstration that the measure is demonstrably necessary to meet a specific need, likely to be effective in meeting that need, proportional in terms of privacy loss versus benefit gained, and that no less privacy-invasive alternative exists ⁸ . Even if the collection, use, and disclosure of biometric information meets this test, consent of the individual is still required except in specific instances outlined under PIPEDA ⁸ .

5.3 Untraceable Biometrics and the Ontario Privacy Commissioner

The Ontario Privacy Commissioner has discussed the development of "untraceable biometrics" as a secure technology that enables processing and use of biometric information without associating it to an identifiable individual. This technology uses a "one-to-one" approach allowing control of biometric information to rest with the individual. It cannot be worked backward to access biometric information about an individual and can be revoked or cancelled if the system is compromised ⁸ .

Despite the existence of untraceable biometric technology, it is rarely used. The Ontario Commissioner has identified various reasons including the newness of the technology, lack of understanding, unsuitability for every context, prohibitive expense, and insufficient pressure from privacy advocates and the public 8 .

5.4 Provincial Privacy Laws

British Columbia's Personal Information Protection Act (PIPA) regulates the flow of personal information within the province. The legislation contains similar requirements to PIPEDA in terms of consent, purpose specification, and security safeguards. Alberta and Quebec have similar legislation 8 .

6. Legal and Regulatory Landscape in the United States

The United States lacks a comprehensive federal privacy law comparable to PIPEDA or the GDPR. Data privacy regulation exists as a mosaic of sector-specific laws at the federal level and state-level regulations 2 .

6.1 Illinois Biometric Information Privacy Act

Illinois became the first state to enact legislation regulating the collection, use, and retention of biometric information with the passage of the Biometric Information Privacy Act (BIPA) in 2008 3 . BIPA makes it illegal for a company to collect an individual's biometric identifier or information unless the company first informs the person in writing, discloses the specific purpose and length of time for which the data is being collected, stored, or used, and obtains written consent 3 .

The term "biometric identifier" is defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" 3 . BIPA further requires the company in possession of the data to protect the security of the information 3 .

Comparison of Key Biometric Privacy Laws in the United States and Canada:

Aspect	Illinois BIPA	Texas CUBI	Washington Law	PIPEDA (Canada)
Year Enacted	2008	2009	2017	2000 (amended)
Scope	Private entities	Commercial entities	Businesses handling	Private sector

Aspect	Illinois BIPA	Texas CUBI	Washington Law	PIPEDA (Canada)
			biometric data	commercial activities
Consent Requirement	Written informed consent	Notice and consent	Notice and consent	Express consent (default)
Private Right of Action	Yes	Limited	Limited	Via Federal Court
Definition of Biometric Identifier	Retina/iris scan, fingerprint, voiceprint, hand/face geometry	Similar to BIPA	"Biological characteristics" including fingerprint, voiceprint, eye retinas, irises	Biometric data considered sensitive personal information
Data Security Requirement	Reasonable standard of care	Prohibition on sale/disclosure	Protection requirements	Safeguards appropriate to sensitivity

6.2 Texas Capture or Use of Biometric Identifiers Act

Texas enacted the Capture or Use of Biometric Identifiers Act (CUBI) in 2009 ³ . The statute requires companies to notify individuals and receive consent before collecting biometric information, but does not specify how notice must be conveyed or how consent must be obtained ³ . The definition of "biometric identifier" is almost identical to that of Illinois BIPA ³ . CUBI precludes a company that possesses biometric data obtained for commercial purposes from selling, leasing, or otherwise disclosing the information unless a limited exception applies ³ .

6.3 Washington Biometric Privacy Law

Washington became the third state to enact a biometric privacy law in May 2017 ³ . The law defines biometric data as that which is "generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual" ³ . The statute requires businesses that collect biometric identifiers to provide

notice and obtain consent before collecting, converting, and storing biometric data for later comparison and matching ³ .

6.4 Legislative Trends

As of mid-2017, five additional states have introduced bills governing the collection, use, and retention of biometric data. Massachusetts considered adding biometric information to its definition of "personal information" ³ . New Hampshire proposed restrictions on businesses that collect, use, or retain biometric data, including creating a private right of action ³ . Alaska proposed heightened consent requirements ³ . Connecticut proposed banning use of facial recognition software for marketing purposes ³ . Montana introduced a bill to impose heightened notice and consent requirements ³ .

6.5 Geolocation Privacy Legislation

The Geolocation Privacy Protection Act (GPPA), which passed both houses of the Illinois legislature in 2017, would prohibit certain tracking of another's location. The GPPA provides that "a private entity may not collect, use, store, or disclose geolocation information from a location-based application on a person's device" unless it first provides notice and receives the person's "affirmative express consent" ³ . Geolocation information is defined as information that is not the contents of a communication, is generated by or derived from the operation of a mobile device, and is sufficient to determine or infer the precise location of that device ³ .

7. Comparative Analysis of Privacy Frameworks

The General Data Protection Regulation (GDPR) of the European Union categorizes facial data as sensitive biometric data under Article 9, imposing stringent requirements for processing ² . In Canada, PIPEDA treats biometric data as sensitive by default. Brazil's LGPD similarly classifies biometric data as sensitive ² .

In the United States, Illinois BIPA requires informed written consent and prohibits data collectors from profiting from biometric data ² . The Federal Trade Commission has warned about misuses of biometric information and harm to consumers ² .

The Office of the Privacy Commissioner of Canada has applied PIPEDA's provisions in several contexts involving biometric data. In one instance, the Commissioner examined the collection by an employer of employee voice recordings to replace passwords for authentication ⁸ . In another, the Commissioner investigated the Law School Admission Council's collection of fingerprints from students taking the Law School Admissions Test ⁸ .

8. Barriers for Vulnerable and Homeless Populations

The systematic review on health and housing experiences of refugees and migrant populations experiencing homelessness reveals significant barriers that would affect adoption of a digital identity application. These findings are directly relevant to the feasibility of a biometric-based digital identity app for homeless populations.

8.1 Barriers to Access

Migrants experiencing homelessness often struggle to meet their housing and health needs and to access essential services because of interpersonal racism, limited proficiency with the local language, lack of financial stability, and family tensions ⁶. Limited language skills negatively affect accessibility to health and social services for migrants, including housing programs ⁶.

Difficulty obtaining employment is frequently reported as a barrier to stable and secure housing ⁶. Being denied work or meaningful opportunities inhibits migrants' pride in being active citizens and affects their personal sense of accomplishment ⁶.

8.2 Discrimination and Systemic Barriers

Refugees experience individual and systemic racism that exacerbate housing instability. Many refugees feel they are turned away from housing and emergency shelters because of their ethnicity, use of welfare cheques, history of trauma, language of origin, temporary resident status, and the presence of children ⁶.

8.3 Mental Health and Trauma

Past trauma worsens the mental health conditions of refugees and other migrants. Premigration and migration exposures of trauma and violence are linked to the initiation or exacerbation of common mental health conditions, including major depressive disorders, generalized anxiety, and posttraumatic stress disorders ⁶. Homelessness after resettlement is a fundamental component that worsens many mental health conditions among migrants ⁶.

8.4 Implications for Digital Identity Application

The barriers identified in the systematic review have direct implications for the feasibility of a biometric-based digital identity application for homeless populations:

Barrier	Implication for Digital Identity App	Mitigation Strategy
Limited language skills	Difficulty understanding consent forms and instructions	Multi-language support, plain language interfaces
Lack of financial stability	No access to smartphones or data plans	Provide low-cost devices, offline functionality
Discrimination	Reluctance to engage with digital systems	Community advocates, trusted intermediaries
Mental health conditions	Difficulty managing credentials and authentication	Assisted custody, recovery mechanisms
Lack of stable housing	Loss of device or credentials	Biometric-only recovery, no-cost replacement
Digital literacy barriers	Difficulty using app features	User-centered design, training programs

9. Security Risks and Biometric Template Protection

Biometric recognition systems are subject to various software-related attacks that pose significant dangers to personal data security. Awareness of these vulnerabilities is often lacking among researchers and biometric stakeholders, potentially leading to serious breaches if unaddressed ¹.

9.1 Types of Biometric Attacks

Attacks on biometric authentication systems can be categorized into presentation attacks and software-related attacks. Presentation attacks require the presentation of fake or fabricated materials to the biometric sensor with the intent of bypassing the authentication module. Software-related attacks are mostly carried out using sophisticated tools and hacking skills to launch attacks at various vulnerable points on the biometric system ¹.

9.2 Inversion Attacks

Inversion attacks involve reconstructing the original biometric sample from stored templates. The template format is an important piece of information that can easily lead to

system compromise when acquired by an adversary. In most circumstances, the format of the templates is either obtained through illegal means or constructed using SDKs that accompany them ¹.

The adoption of NIST or ISO standard templates, which enhance interoperability among systems and applications, may also pose a security risk. A potential adversary might use this public information to recreate valid, compliant templates and conduct attacks against the system ¹.

9.3 Protection Mechanisms

Over the last two decades, researchers have proposed different methods to mitigate some attacks, while a large number of existing attacks remain unattended ¹. Biometric template protection mechanisms fall into two main categories: cancelable biometrics and biometric cryptosystems.

Cancelable biometrics transform biometric templates using non-invertible functions, ensuring that unprotected templates are neither used for verification purposes nor stored in the system database. This approach ensures that no biometric information will be revealed in the event of a data breach ¹.

Biometric cryptosystems merge cryptography and biometrics to generate a secure sketch stored as auxiliary data. The authentication process involves an indirect comparison where the validity of a key obtained from the biometric probe is verified through the auxiliary data ¹.

The ISO/IEC, ANSI/NIST, and EU-GDPR data protection standards stipulate that protected templates must adhere to cancelability/revocability, non-invertibility, and unlinkability criteria ¹.

10. Self-Sovereign Identity as an Alternative Paradigm

Self-sovereign identity (SSI) offers an alternative approach to biometric-based identity systems. The concept is intended to preserve the right for selective disclosure of different aspects of one's identity in different domains and contextual settings. This right should apply regardless of whether these aspects have been issued by a particular government, company, or organization ⁷.

10.1 Core Principles of Self-Sovereign Identity

Ten core principles guide self-sovereign identity systems 7 :

Principle	Description
Existence	Users must have an independent existence
Control	Individuals must control their identities
Access	Individuals must have access to all data related to their identities
Transparency	Systems must be open and transparent
Persistence	Identities must be long-lived
Portability	Information must be transportable
Interoperability	Identities should be widely usable
Consent	Individuals must agree to the use of their identities
Minimization	Disclosure must be limited to the minimum necessary
Protection	User rights must be protected

10.2 Credential-Based Identity Systems

An alternative to identity systems based on unique and singular identifiers is a claims and credentials-based system. In such a system, identity is not reduced to an authoritative identifier such as biometric or government-issued identification numbers. Instead, identity is defined through a network of claims and credentials based on a web of trust authentication 7 .

A credentials-based system better mirrors the multifaceted nature of human identity, allowing different profiles and personas to emerge through combinations of different claims and credentials depending on the use cases 7 . A profile appropriate for a loan application would be different from a profile appropriate for accessing social services.

10.3 Case Studies

The World Food Programme's Building Blocks program uses blockchain-based identity for delivering cash aid to refugees in Jordan ⁷ . The program channels entitlements to unified blockchain wallets for each beneficiary, creating portable financial transaction histories. If a Syrian refugee returns home, she could use the data generated in Jordan to get a small business loan in Syria ⁷ .

Kiva is building an identity protocol based on the DID and credentials model using Hyperledger Indy as the underlying blockchain layer. It relies on a credential-based identity system where the basic identifier is a public/private key pair, to which multiple claims and attestations can be associated ⁷ .

10.4 Infrastructure Requirements

A true self-sovereign identity system requires a certain level of infrastructure, primarily high penetration of affordable smartphones that can securely store private keys and reliable connectivity ⁷ . The lack of proper connectivity and hardware infrastructure is a key obstacle to overcome in the roadmap toward self-sovereign identity ⁷ .

11. Feasibility Analysis for a Vancouver Pilot Project

11.1 Legal Feasibility

A pilot project in Vancouver would operate under British Columbia's Personal Information Protection Act (PIPA) and the federal PIPEDA. The application must satisfy the four-part test for biometric collection: demonstrable necessity, effectiveness, minimal intrusiveness, and proportionality ⁸ .

The application must also comply with PIPEDA's requirement for express consent for biometric data processing. Consent must be explicit, informed, specific to biometrics, integrated into user flows, and renewable ² . Organizations must provide opt-out options and alternatives, especially when biometrics are not essential to the service ² .

11.2 Technical Feasibility

The technical architecture would need to satisfy NIST AAL2 requirements for most applications, with AAL3 for high-security functions such as voting. The system must:

- Use biometrics only as part of multi-factor authentication with a physical authenticator ⁴
- Achieve a False Match Rate of 1 in 1000 or better ⁴

- Limit consecutive failed attempts to no more than five 4
- Implement Presentation Attack Detection with at least 90% resistance 4
- Store biometric templates only on the device, not on central servers
- Enable revocation and replacement of compromised credentials

11.3 Infrastructure Requirements

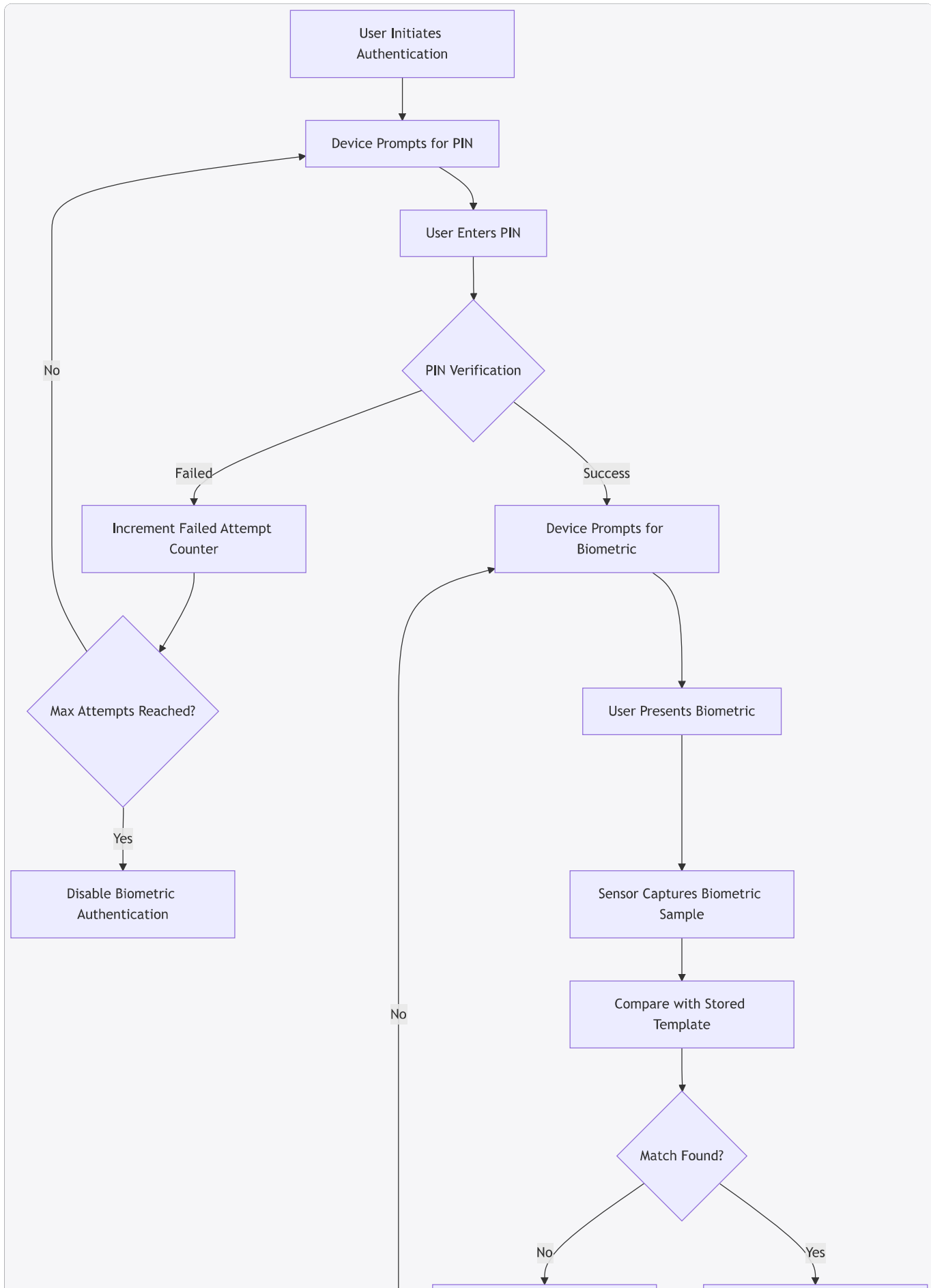
The pilot would require partnerships with organizations serving homeless populations to provide:

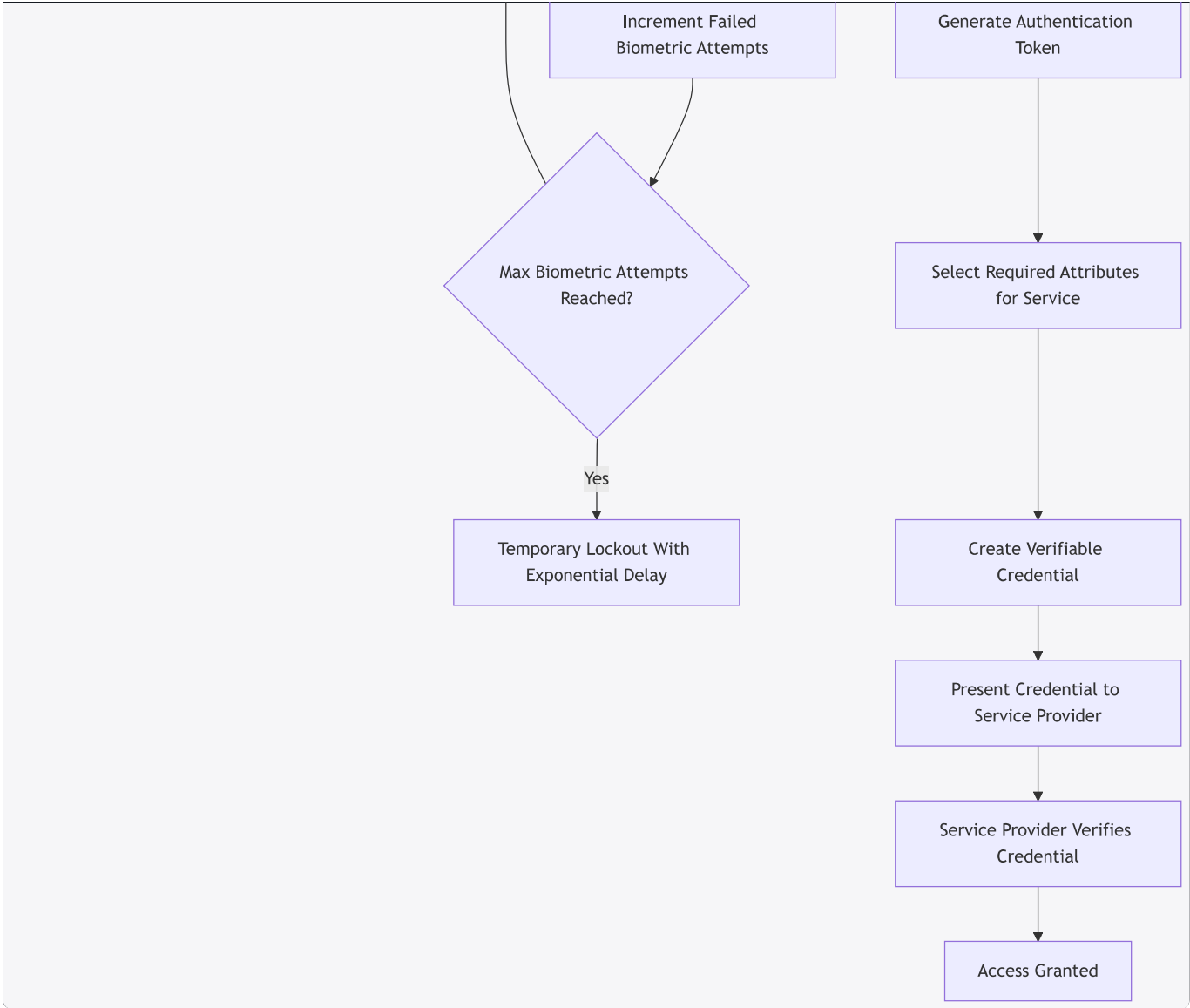
- Access to smartphones or low-cost devices
- Internet connectivity or offline functionality
- Training and support for users with limited digital literacy
- Community advocates to assist with enrollment and authentication

11.4 Integration with Banking and Voting

The application would need to comply with existing regulatory requirements for each use case:

Authentication Flow for a Biometric Digital Identity Application:





Use Case	Regulatory Considerations	Technical Requirements
Banking	FINTRAC compliance, KYC/AML	AAL2 authentication, identity proofing at IAL2
Voting	Election integrity, one person one vote	AAL3 authentication, uniqueness guarantee
Government Services	PIPA/PIPEDA compliance, FOIPPA	AAL2 authentication, minimum data disclosure
Healthcare	PHIPA compliance, consent management	AAL2 authentication, role-based access control

12. Pathways for North American Expansion

12.1 Regulatory Challenges

Expansion across North America would require navigating a complex patchwork of state-level biometric privacy laws. The most significant challenge would be compliance with Illinois BIPA, which requires written informed consent and creates a private right of action ³. Texas CUBI and Washington law have similar but not identical requirements ³.

The varying state laws impose different requirements for consent, data retention, data sharing, and security safeguards. A single application that complies with all applicable laws would need to implement the most restrictive requirements across all jurisdictions.

12.2 Interoperability Requirements

Interoperability and standardization will be important for scale, but the success of a particular identity application will depend on how its deployment is tailored to the use cases and local conditions ⁷. The application would need to:

- Support multiple consent frameworks
- Adapt to different state-level requirements
- Enable selective disclosure of attributes based on jurisdictional requirements
- Maintain compliance with varying data retention and deletion requirements

12.3 Cross-Border Enforcement Challenges

The internet-driven nature of data collection often involves entities operating across multiple jurisdictions, complicating enforcement efforts as national data protection authorities may struggle to assert jurisdiction over foreign companies ². The global reach of data collection often outpaces the territorial limitations of existing laws ².

13. Proposed Framework and Recommendations

Based on the analysis of technical, legal, and social factors, we propose the following framework for developing and deploying a biometric-based digital identity application:

13.1 Technical Architecture

The application should adopt a self-sovereign identity approach using verifiable credentials and decentralized identifiers. This architecture provides flexibility and efficiency while contributing to securing fundamental human rights ⁷. The system should incorporate:

- On-device biometric storage and matching
- Decentralized identifiers for portability
- Verifiable credentials for attribute attestation
- Zero-knowledge proofs for minimal data disclosure
- Secure backup and recovery mechanisms

13.2 Privacy Implementation

Privacy-by-design principles must be incorporated from the outset. The system should:

- Use untraceable biometric technology where the original data cannot be recreated from stored information 8
- Implement one-to-one verification rather than one-to-many identification
- Provide clear, meaningful feedback on remaining allowed attempts 4
- Allow users to select the modality they are most comfortable with for authentication 4

13.3 Inclusion Measures

To address the needs of homeless and vulnerable populations, the application should:

- Provide alternatives to smartphone-based authentication
- Offer assisted enrollment and authentication through community advocates 6
- Implement language-accessible interfaces
- Provide offline functionality for areas without reliable connectivity
- Establish partnerships with shelters and service providers

13.4 Legal Compliance

The application must ensure compliance with all applicable laws by:

- Obtaining express, informed, and granular consent
- Providing clear privacy notices
- Implementing appropriate security safeguards
- Enabling data deletion upon consent withdrawal
- Conducting privacy impact assessments

14. Conclusion

The feasibility of a standardized biometric-based digital identity application replacing physical identification cards depends on resolving significant technical, legal, and social challenges. A pilot project in Vancouver is viable with appropriate privacy-by-design principles, self-sovereign identity architecture, and partnerships with organizations serving vulnerable populations. However, expansion across North America faces substantial hurdles due to fragmented state-level biometric privacy laws, security vulnerabilities inherent in biometric systems, and infrastructure requirements that may exclude homeless populations.

The key findings of this analysis can be summarized as follows:

Dimension	Assessment	Recommendation
Technical Feasibility	High with existing technology	Implement SSI architecture with on-device biometrics
Legal Feasibility (Canada)	Moderate	Satisfy PIPEDA four-part test; comply with PIPA in BC
Legal Feasibility (USA)	Low under current patchwork	Require state-specific compliance; advocate for federal legislation
Inclusion for Homeless	Challenging but addressable	Partner with service providers; provide alternative access methods
Security Robustness	Moderate	Implement protection mechanisms; plan for revocation
Scalability	High if interoperability standards adopted	Adopt DIDs and verifiable credential standards

The development of such an application should proceed incrementally, beginning with a carefully designed pilot in Vancouver that addresses the specific needs of homeless populations while testing compliance with Canadian privacy legislation. Expansion to other jurisdictions should follow successful demonstration of the pilot's effectiveness, security, and inclusion outcomes. The long-term potential of biometric-based digital identity remains high, particularly for vulnerable populations who lack traditional identification documents, but realizing this potential requires careful attention to the barriers and risks identified in this analysis.

