HC BILL 28-16

National ID Act of 2026

An Act to establish National ID credentials and a refugee identification class; provide for civil registration, legal names, credential security, flexible credential designs and variants, digital registration and verification, continuous credential histories and issuance fees; establish security standards for official digital services; require identification for specified electoral and firearms purposes, subject to public approval; and amend Titles 2 and 7 of the Civil Code of the Totemian Empire.

BILL · 28TH TOTEMIAN PARLIAMENT

Introduced October 31st, 2026

Nuxart (Member of the House of Commons, The Birthday Party)

National ID Act of 2026

Introduced By: Nuxart (The Birthday Party)

Date: October 31st, 2026

Be it enacted by the Parliament of the Totemian Empire, duly assembled, with the assent of the Emperor, as follows:

Purpose and Scope

An Act to establish National ID credentials and a refugee identification class; provide for civil registration, legal names, credential security, flexible credential designs and variants, digital registration and verification, continuous credential histories and issuance fees; establish security standards for official digital services; require identification for specified electoral and firearms purposes, subject to public approval; and amend Titles 2 and 7 of the Civil Code of the Totemian Empire.

Section 1: Short Title

This Act may be cited as the National ID Act of 2026.

Section 2: Civil Registry

Title 2, Chapter 9, Article 6, Section 3 of the Civil Code is amended to read:

Section 3: Civil Registry

The Office shall maintain the Civil Registry for civil-status records assigned to the Ministry by law, including civil marriages and divorces, citizenship applications and oaths, and other records concerning the legal status of natural persons.

References in existing law to the Imperial Civil Registry shall be construed as references to the Civil Registry. Its records, functions and competent authority shall continue.

Section 3: Civil Registration Functions and Personnel

Title 2, Chapter 9, Article 6, Section 2 of the Civil Code is amended to read:

Section 2: Leadership and Personnel

The Office shall be led by the Registrar-General of the Totemian Empire. The Deputy Registrar-General shall be second in command. Both officers shall be appointed and removable at will by the Minister of Interior unless the Emperor directs otherwise. Other personnel may be styled Civil Registrars or receive functional titles by Policy Order.

The Registrar-General shall direct the Office's national registration functions, supervise its personnel, ensure the accuracy and security of its records, and report to the Minister of Interior. The Deputy Registrar-General shall assist the Registrar-General and act during absence or incapacity, subject to a contrary lawful direction.

The Minister may appoint or assign Senior Civil Registrars to supervise specified registration work, review applications and corrections, and oversee Civil Registrars within their assigned functions. Civil Registrars shall receive and examine filings, verify required particulars, maintain records and perform authorized registration functions. Supervisory grades and functional assignments shall be recorded without creating a separate Office or Administration.

Title 2, Chapter 9, Article 6 is amended by inserting Sections 7 through 10 immediately after Section 6, to read:

Section 7: Civil Registration and National ID Functions

The Office shall maintain the Civil Registry as the authoritative register of identity and civil-status particulars assigned to it by law. It shall register legal names and name changes, gender, residence, citizenship records, competent refuge determinations, civil marriages and divorces, and births, deaths, parentage and other civil-status events established under applicable law. Entries shall identify the supporting application, instrument or competent determination.

The Office shall administer National ID registration, issuance, renewal, replacement, correction, suspension and revocation; maintain authoritative identity and credential records; and provide verification services under Articles 8 through 12 of this Chapter. It shall prepare and preserve citizenship applications and oaths for determination under the Constitution and other law. Marriage, divorce and fiduciary registration shall continue under their governing provisions.

Section 8: Functional Assignments

The Registrar-General shall assign responsibility for application processing and identity verification, civil-status entries and corrections, credential issuance and authentication security, and record custody and audit. A lawful assignment may be held with another registration function where the holder can perform both competently. Functional assignments shall specify the permitted actions and access to protected records.

A person acting as an Authorized Registration Processor shall retain their substantive office or position. The system shall record the actual person, office and authority under which an action is performed. Hierarchical competence, acting authority and interorgan assistance shall operate under Title 2, Chapter 4.

Section 9: Record Integrity and Coordination

Each person shall have a distinct registry record linked to their National ID number and credential history. The Office shall check duplicate and conflicting entries, preserve supporting records and previous versions, and record the actor, time, reason and authority for material changes. A correction shall preserve the history necessary to explain the current entry.

The Office shall supply certified extracts and verification results to the holder or a lawfully authorized requester. It shall coordinate citizenship and identity information with the National Electoral Administration, residence information with Territorial Administration, and other particulars with the competent state organ. The source authority for an underlying legal determination shall be preserved.

Section 10: Service Procedures and Supervision

The Minister shall prescribe accessible procedures for applications, appointments where needed, correction requests, certified extracts, record access, referrals and administrative review. The Registrar-General shall publish the available services and requirements, supervise timely handling, and report material backlogs, errors and security incidents to the Minister.

An adverse registration decision shall identify its reasons and the available review procedure. A person seeking correction shall be able to submit supporting information and receive the recorded outcome. Record access and disclosure shall comply with Article 7 of this Chapter and the protections applicable to the particular record.

Section 4: National Identity Registration and Credentials

Title 2, Chapter 9 is amended by inserting Article 8 immediately after Article 7 and before Chapter 10, to read:

Article 8: National Identity Registration and Credentials

Section 1: Registration and General Recommendation

Every citizen should obtain and maintain an active National ID. The Office of Civil Registration shall receive applications from citizens and persons lawfully granted refuge in the Totemian Empire, and from other persons made eligible by law.

Section 2: Authorized Registration Processor

An Authorized Registration Processor is a person lawfully exercising a function in receiving, examining, processing, deciding or issuing a National ID application by virtue of office, acting authority, hierarchical competence, lawful assignment or permitted interorgan assistance. A Processor shall act within that competence. The designation is functional and shall not establish a separate office.

Section 3: Credential Classes

The following classes shall be available:

(A) Class A: an account-linked credential connected to the holder's Totemian digital account and subject to the Integrated Digital Tier requirements;

(B) Class B: a credential maintained in the Civil Registry without a linked Totemian digital account;

(C) Class R: a Refugee or Resident Identification credential identifying a person whose refuge has been granted by competent authority and who is not recorded as a Totemian citizen.

A Class R credential may be account-linked or non-account. An account-linked Class R credential shall satisfy the Integrated Digital Tier requirements. The credential record shall distinguish legal status, class and integration tier. Refugee status shall be supported by the competent determination, including its reference, effective date and any lawful conditions.

Section 4: Required Particulars

An application must contain the applicant's first name, designated surname, gender, residence, identification portrait and signature. The record shall include the identity of the Processor, the decision and the date and time of registration and issuance. Applicable citizenship or refuge status shall be verified against the competent records.

Section 5: Legal Name and Additional Name Components

The legal name required for identification shall consist of the first name and designated surname recorded in the Civil Registry. A surname may be an inherited family name or a parent-derived surname. An applicant may also register additional given names, additional surnames, patronymics, matronymics, ancestral or lineage names, clan or house names and other personal name components. A generational suffix may be registered.

Additional components shall be recorded separately by type, exact text and confirmed position in the full registered name. Particles and lineage connectors shall be preserved with the relevant component. A component already entered as the surname shall not be duplicated merely to classify it. The full registered name shall preserve the confirmed spelling and order.

Honorifics, public offices, parliamentary designations, academic or professional titles, military or religious ranks and political party positions shall not form part of the registered legal name. Account display names shall not be divided automatically into legal-name fields.

Unless another law expressly requires the full registered name, the recorded first name and designated surname shall satisfy a legal-name requirement. Additional components and suffixes may be included only as recorded. A correction or change shall be processed through the Office and preserved in the record history.

Section 6: Gender

The field shall be designated Gender. Male and Female must be available. The Minister of Interior may prescribe additional entries and procedures for recording and correcting gender by Policy Order.

Section 7: Residence

Residence shall be recorded through the applicable subnational government, province or district, settlement and optional street address. Territorial entries shall correspond to authoritative territorial records. Where a level is inapplicable, it shall be omitted.

The displayed residence shall place the settlement first, the province or district next where recorded, and the subnational government last. An optional street address shall be retained in the protected record and displayed where the holder requests it or law requires it.

Section 8: Portrait and Signature

The applicant must provide an identification portrait and specimen signature. Before issuance, the Processor shall inspect the portrait for suitability as an identification image and record approval or the reason for requiring another image. The Minister may prescribe consistent requirements for clarity, framing, legibility and appropriate content.

The signature shall be associated with the applicant, its capture or submission date and the accepting Processor. Reuse for a renewed or replacement credential shall require the holder's confirmation. A replacement shall preserve the previous signature and record the actor, time and reason for the change.

Section 9: Person and Credential Identifiers

The Office shall assign a unique National ID number to each registered person and an independently distinguishable reference to each credential issuance. The National ID number shall remain associated with that person through renewal, replacement, name change or movement between classes. A new issuance shall have its own credential and seal references.

The Office shall retain the version of the allocation scheme and the issuance inputs necessary to verify the number's components. A random component shall be verified against the issuance record. Subsequent changes to personal particulars shall be recorded without silently recomputing the original number.

Section 10: Validity

A credential shall expire automatically at the end of its displayed expiry date, calculated 6 calendar months after issuance. If the corresponding numbered day does not exist in the expiry month, the last day of that month shall be used. The Minister shall prescribe and publish the governing system time zone. Issue and expiry dates shall be generated by the issuing service.

Section 11: Examination and Decision

The Processor shall examine completeness, identity consistency, eligibility, duplicate records, portrait approval, signature acceptance and completion of the required PIN and passkey enrollment. Issuance shall be blocked while a required condition, including payment of the applicable fee under Section 13, remains unsatisfied. A refusal or request for correction shall state its reasons in the application record and be communicated to the applicant.

Section 12: Refugee Status and Legal Qualifications

A Class R record shall distinguish an effective grant of refuge from an application awaiting determination. Eligibility for voting, candidacy, employment, property, services and other activities shall be determined under the law governing the activity. A verification service shall apply the holder's recorded status and any competent restrictions to the particular requested use.

Section 13: National ID Issuance Fee

The fee for each initial, renewed or holder-requested replacement National ID shall be 1,000 SL. The Central Revenue Administration shall collect the fee after the application is approved as ready for issuance and credit it to the Collections Fund. The issuing service shall verify the payment reference before issuing the credential and associate it with that issuance.

No additional fee shall be charged merely for linking an existing registry record to an account, retrieving credential history or correcting an error attributable to the issuing authority. A replacement required solely to correct such an error shall be issued without charge. A rejected application shall incur no issuance fee. If a paid issuance cannot be completed, the payment shall be applied to the same completed issuance or refunded through the Central Revenue Administration. A repeated submission shall not create a duplicate charge.

Section 5: Credential Form and Eagle Authentication Seal

Title 2, Chapter 9 is amended by inserting Article 9 immediately after Article 8 as inserted by this Act and before Chapter 10, to read:

Article 9: Credential Form and Eagle Authentication Seal

Section 1: Required Display

Every National ID shall display its class, legal name, gender, residence, approved portrait, specimen signature, National ID number, credential reference, issuing authority, issue date and expiry date. A Refugee Identification credential shall display that designation clearly. Every National ID shall prominently display the official national flag of the Totemian Empire, separately from its required Eagle Authentication Seal. This requirement applies to physical and digital credentials and to all approved variants. The flag shall remain recognizable and shall not be omitted, replaced, obscured or materially altered. The Ministry may prescribe additional lawful fields.

The credential shall use English and Totemic, with corresponding Totemic text larger than the English text. Physical-card issue and expiry labels shall include ISS and EXP. Dates shall use 2 digits for the day, the 3-letter month abbreviation and 4 digits for the year, separated by spaces. The month abbreviations shall be JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV and DEC. Totemic labels shall precede corresponding English labels and use a nominal type size at least 20% larger, with comparable weight and contrast. The approved layout shall state physical dimensions in millimetres and digital dimensions in pixels and shall demonstrate legibility at the

intended card size. A shared date value may be displayed once. Absolute point sizes shall be set in the approved layout rather than copied from an enlarged screen preview.

For example, a credential issued on October 31st, 2026 shall display “ISS 31 OCT 2026” and “EXP 30 APR 2027”. An equivalent full-date digital view may display “Date of issue: October 31st, 2026” and “Date of expiry: April 30th, 2027”. These examples specify the format; each credential shall use its actual issue and expiry dates. Corresponding Totemic labels shall use the officially prescribed translations and appear larger than the English labels. The residence order shall comply with Article 8, Section 7.

Section 2: Eagle Authentication Seal

Every credential shall carry the approved holographic eagle emblem and a credential-specific machine-readable authentication layer, together designated the Eagle Authentication Seal (EAS). The public-facing eagle shall remain recognizable. The machine-readable layer shall contain authenticated information bound to the particular credential issuance and recoverable through the approved reader profile.

A physical credential shall use the prescribed optically variable holographic device and covert reading feature. A digital credential shall reproduce the approved holographic visual effect and provide the signed machine-readable layer in its native presentation. Reader and carrier requirements shall be prescribed for each medium.

Section 3: Authenticated Seal Information

The seal shall authenticate the issuing authority, profile version, trusted signing-key reference, National ID number, credential and seal references, class, integration tier, issue date and expiry date. It shall also bind the credential to its approved issuance particulars, including legal name, gender, residence, portrait and specimen signature, by signed data or an authenticated reference and integrity value for the protected issuance record.

The issuing authority shall digitally sign the authenticated information. Verifiers shall obtain trusted issuer keys through an authenticated trust service. A key supplied by the presented credential alone shall not establish trust.

Section 4: Visible and Concealed Features

The prescribed security profile shall specify the eagle's visible features, concealed encoding, capture conditions, decoding requirements, comparison procedure and acceptable tolerances. Physical profiles shall identify the necessary optical equipment and illumination. Digital profiles shall define the native authenticated presentation and permitted image transformations.

The seal must be validated at the final display or print size before a profile is approved. A generic image, a matching number or an unverified hidden pattern shall not satisfy the authentication requirement.

Section 5: Protected Secrets

PINs, PIN verifiers, private signing keys, passkey private keys and recovery secrets shall not be encoded in the credential or seal. Access to protected identity particulars shall remain subject to the lawful purpose and permissions of the requesting service.

Section 6: Integrity and Replacement

The seal shall permit detection of changes to authenticated credential particulars. A copied seal placed on a credential with inconsistent particulars shall fail verification. Where a change requires a new authenticated issuance record, the Office shall issue a replacement credential and seal and update the status of the superseded issuance.

Section 7: Technical Profiles

Approved versioned profiles shall be published for credential layout, machine-readable carriers, signatures, trust-key distribution, optical features, record bindings, interoperability and conformance testing. Profiles shall state their supported media and verification capabilities. Profiles requiring protected-chip or other active anti-cloning authentication shall specify a fresh cryptographic challenge and protected credential key.

Technical profiles shall preserve the mandatory verification stages under Article 11. Sensitive manufacturing masters and signing keys shall be protected by the issuing authority.

Section 8: Initial Cryptographic Seal Profile

The initial digital profile shall be designated EAS-PNG-1. It shall encode its signed payload using the core deterministic CBOR requirements in RFC 8949, Section 4.2.1, and the tagged COSE_Sign1 structure in RFC 9052. The initial signature algorithm shall be ECDSA on the P-256 curve with SHA-256, designated ES256 under RFC 9053. Implementations shall use maintained cryptographic libraries and validate the key type, curve, algorithm and signature structure.

The algorithm and signing-key identifier shall be in the protected COSE headers. The unprotected header map and external authenticated data shall be empty. The payload shall be included in the signed object, not detached. Duplicate map keys, indefinite-length encodings, unsupported algorithms and nonconforming structures shall be rejected.

An authenticated issuer-key register shall be maintained identifying each key's issuer, identifier, algorithm, validity interval and status. Verification keys shall be obtained from that register or an authenticated, current distribution of it. A credential-supplied key or address shall not establish issuer trust. Key retirement and revocation shall be distinguished so a normal rotation does not erase the ability to verify preserved history.

Section 9: Signed Payload and Issuance Snapshot

The EAS-PNG-1 payload shall be a deterministic CBOR map using the following unsigned integer field numbers:

(A) 1: profile version, as the integer 1;

(B) 2: issuing-authority identifier, as text;

(C) 3: signing-key identifier, as a byte string matching the protected header;

(D) 4: permanent registry-person reference, as an opaque text identifier;

(E) 5: National ID number, as text;

(F) 6: distinct credential-issuance reference, as text;

(G) 7: seal reference, as 16 bytes generated by a cryptographically secure random source;

(H) 8: credential class, as the text A, B or R;

(I) 9: integration tier, as the integer 1 for Integrated Digital Tier or 0 for non-account;

(J) 10: issue time, as an integer number of seconds since January 1st, 1970 at 00:00 UTC;

(K) 11: expiry time, in the same representation, identifying the first instant at which the credential is expired;

(L) 12: the 32-byte SHA-256 digest of the immutable issuance snapshot;

(M) 13: the 32-byte SHA-256 digest of the credential image under Section 10;

(N) 14: approved layout-profile identifier, as text.

All 14 fields shall be present. Text shall use UTF-8 in Unicode normalization form C. Times shall agree with the recorded issue and expiry dates and the governing system time zone. The signed class, tier, layout and identifiers shall match the selected issuance record. The seal reference shall not be reused for a different issuance.

The immutable issuance snapshot shall contain the approved displayed particulars, full registered name and component order, gender, residence, portrait and specimen-signature references and integrity values, class, tier, issue and expiry particulars, identifiers, and allocation-scheme version. The layout profile shall publish its exact deterministic CBOR field schema before issuance under that profile. The snapshot and its digest shall be preserved with the credential history. A later live-record correction shall not overwrite that snapshot.

Section 10: Concealed Native PNG Carrier

EAS-PNG-1 shall use a single-frame, lossless PNG image with 8-bit red, green and blue channels in sRGB. Its pixels shall be opaque. The approved layout shall fix the image dimensions and a rectangular machine-reading region within the eagle security panel. The issuance record and authenticated layout register shall identify that region; its position shall not be accepted solely from an untrusted uploaded image.

The concealed carrier shall use the least significant bit of the blue channel of each pixel in that region. Pixels shall be read from left to right, row by row from top to bottom. Successive groups of 8 bits shall form bytes, with the first bit as the most significant bit. The carrier shall begin with a 1-byte version value of 1, followed by a 4-byte unsigned big-endian length for the COSE object and then that complete object. Remaining carrier bits shall be zero. The issuer shall verify that the object fits the region before issuance. The reader shall enforce the region's capacity and a maximum object length of 4,096 bytes.

Before computing the credential-image digest, the issuer shall set the blue-channel least significant bit to zero throughout the carrier region. The digest input shall be the image width and height, each represented by 4 unsigned big-endian bytes, followed by the red, green and blue bytes of every pixel in row order. It shall exclude file metadata and compression bytes. The reader shall perform the same operation on the decoded native pixels before comparison. Display colour correction, scaling and other image transformations shall not be applied to the decoded pixels used for this check.

The issuer shall render the complete card, compute the snapshot and image digests, construct and sign the payload, embed the signed object in the carrier and perform a verification readback before releasing the file. A reader shall extract the carrier, validate its structure, verify the trusted issuer signature and compare both digests with the presented native image and protected issuance snapshot. Each comparison must succeed.

Section 11: Tampering and Presentation Controls

A valid number and visually plausible eagle shall not satisfy EAS verification. An altered name, portrait, signature, date, residence or other rendered image content shall cause an image-digest mismatch under EAS-PNG-1. Moving a genuine seal onto a different card shall fail the signed-identifier, snapshot or image comparison. Failure at this stage shall block completion of NCVS.

EAS-PNG-1 shall verify the original native PNG. Screenshots, resizing, lossy conversion and camera or print scans shall be processed only under a separately approved profile specifying its carrier, capture tolerances, authenticated data and comparison procedure. The digital service shall provide an original-file download and a native-file verification route. A transformation or capture failure shall be recorded as such and shall not by itself establish criminal forgery.

A fully intact copy remains a copy of an authentic credential; holder PIN and required passkey verification shall remain necessary for use. An image carrier shall not be represented as proof of physical-card possession. A physical holographic profile shall define its optical feature, illumination, reader calibration and credential-binding procedure before deployment.

Section 12: Interoperability and Profile Changes

A developer specification and test vectors shall be published for the payload, snapshot schema, image carrier, signatures, layout coordinates and verification outcomes. Tests shall cover a genuine credential, altered fields, transplanted seals, unknown keys, wrong algorithms, malformed or oversized payloads, replaced credentials, transformed images and replayed holder authentication. Protected production keys and personal records shall not be included in public test material.

A later technical-profile version may be approved and published in accordance with law after documented security and interoperability review. The approval shall identify the replacement algorithms and carrier rules, transition dates, accepted profiles and treatment of existing credentials. It shall preserve issuer authentication, binding to the presented credential, unique issuance references and the mandatory NCVS stages. A reader shall reject an unknown or unsupported profile rather than assume success.

Section 13: Authorized Designs and Variants

The Emperor may, after consultation with the Minister of Interior and the Registrar-General, authorize, revise, or discontinue standard and special National ID designs and variants by Imperial Order. Any person, organization, or state organ may propose a design through the existing Office of Civil Registration. Proposals may concern artistic, cultural, historical, civic, regional, institutional, commemorative, or any other lawful subject. These categories are illustrative and shall not restrict the approval of further designs.

The Office shall present proposals through the Minister of Interior for Imperial consideration, together with advice on legibility, security, accessibility and practical implementation. The Emperor may approve a design, authorize a series of related designs, require adjustments, specify its period of availability, or decline it. Neither a separate Act of Parliament nor a fixed sponsorship payment, minimum number of supporters, or separate administrative body shall be required for individual approvals. Parliament may by Act prescribe mandatory design standards, direct the issuance of particular designs or variants, or govern their availability. An Imperial Order remains subject to those Acts.

Every design and variant shall retain the credential's existing class, legal effect, validity, mandatory identity particulars, official national flag of the Totemian Empire, and Eagle Authentication Seal. The flag and seal shall remain recognizable and shall not be omitted, replaced, obscured or materially altered. Artwork, colors, typography, layout and presentation may otherwise vary, provided that mandatory information remains legible and all applicable authentication and security requirements are satisfied. Each approved layout shall be identifiable in its authenticated layout profile and official issuance records.

The Office of Civil Registration shall receive proposals, implement approved designs, and issue credentials through its existing functions. The Minister of Interior may publish ordinary application, technical and production procedures consistent with this Article. Designs may be permanent, temporary, limited to an occasion, or available to holders meeting lawful eligibility conditions. A holder may select among available designs for the holder's credential class. A design variant shall not create a new credential

class, a separate governmental body, or any additional compulsory issuance fee.

Section 6: Digital Registration and Automatic Retrieval

Title 2, Chapter 9 is amended by inserting Article 10 immediately after Article 9 as inserted by this Act and before Chapter 10, to read:

Article 10: Digital Registration and Authoritative Record Prefill

Section 1: Integrated Registration System

The digital registration system for the Integrated Digital Tier shall comply with this Article. Access to the internal fillable application shall be limited to Authorized Registration Processors acting within their permissions. The Processor shall obtain required answers and confirmations from the applicant.

Section 2: Authoritative Record Prefill

Authoritative Record Prefill (ARP) means automatic retrieval and population of applicable application fields from designated authoritative Totemian records. Upon confirmed selection of the intended person or account, the system shall retrieve and populate available particulars automatically. Ordinary registration shall not require a separate request for each available field or retyping of an available authoritative value.

Section 3: Sources and Identification

The selected account shall be linked by a stable system identifier. Search text alone shall not create the link. Legal names shall be retrieved from dedicated legal-name records, legal status from the competent status record, and residence from the designated residence and territorial records. Verified external account links may be retrieved where lawfully available.

Section 4: Missing and Conflicting Information

The system shall distinguish authoritative retrieval, imported information awaiting confirmation, manual entry, missing information, conflict and source-service failure. It shall identify the source and retrieval time of prefilled particulars. Missing particulars shall be obtained from the applicant through the appropriate procedure. An unavailable fact shall not be replaced with an inferred gender, residence, name or legal status.

Section 5: Corrections and Refresh

A correction shall preserve its source, actor, time and reason. Refresh shall not silently overwrite a manual correction or unresolved discrepancy. Changing the selected applicant shall clear the previous applicant's particulars, approvals and enrollment references. Delayed responses concerning the previous applicant shall be discarded.

Amendment of an application shall not amend a separate authoritative register without the competence and procedure required for that register. Material source changes before issuance shall return the affected particulars for review.

Section 6: Name Fields and Review

The ordinary name view shall contain first name, surname and optional suffix. An expandable area shall permit additional typed name components and their confirmed order. Existing additional components retrieved through ARP shall be shown automatically. The system shall display the full registered name for confirmation and preserve meaningful spelling, scripts, accents, punctuation, particles and order. Overlong particulars shall not be silently truncated.

Section 7: Automated Issuance Functions

The service shall generate issuance and expiry dates, allocate or retrieve identifiers, check duplicate credentials and required enrollment, validate territorial relationships, record the deciding Processor and preserve the decision. Repeated submission of the same issuance request shall recover the recorded result rather than issue duplicate credentials.

Section 8: Server Enforcement and Standards

The issuing service shall enforce required fields, lawful permissions, approvals and enrollment conditions independently of the visible interface. Field definitions, source mappings, correction procedures, accessible review controls, failure handling and conformance tests shall be documented and implemented. The Office shall confirm the registry meanings, required particulars and administrative permissions. Required automatic functions shall operate by default.

Section 7: National Credential Verification Standard

Title 2, Chapter 9 is amended by inserting Article 11 immediately after Article 10 as inserted by this Act and before Chapter 10, to read:

Article 11: National Credential Verification Standard

Section 1: Mandatory Sequence

The National Credential Verification Standard (NCVS) shall govern automated verification of National IDs. The service shall perform the following stages in order:

(A) National ID number lookup;

(B) issuance consistency;

(C) Eagle Authentication Seal verification;

(D) holder PIN verification;

(E) holder passkey verification where required by the integration tier;

(F) current validity and permission for the requested use.

A terminal defect may end the attempt earlier. No successful result shall be issued while an applicable stage remains unsatisfied. Preliminary status checks may reject an unusable credential but shall not replace the final check.

Section 2: Number Lookup and Issuance Consistency

The service shall locate the authoritative issuance record, validate the number under its recorded allocation scheme, and compare the documented components with the credential as issued. Derived components shall be checked against their issuance inputs and random components against their stored values. Existence of a matching number shall not establish credential authenticity.

Section 3: Eagle Authentication

The service shall inspect the required visible eagle features, recover its machine-readable authentication information, verify the issuer's signature and trusted key status, and compare authenticated particulars with the presented credential and issuance record. The service shall apply the approved media profile and comparison tolerances. An unreadable required feature shall remain unresolved until successfully recaptured or examined through a lawfully prescribed alternative procedure.

Section 4: Holder PIN

Every credential must have a holder-selected PIN consisting of 8 through 12 digits from 0 through 9. The service shall reject commonly used or readily predictable PINs and require private entry through a protected channel. The PIN shall not be displayed to the Processor, printed on the credential or included in ordinary records or logs.

The verifier shall apply increasing delays after unsuccessful attempts and suspend PIN verification after 10 consecutive failures pending secure recovery. Where verification is central, the service shall protect the verifier with a unique salt, a suitably costly one-way derivation and additional secret protection against offline guessing. Transmission shall be protected against interception.

Section 5: Integrated Digital Tier Passkey

An account-linked credential must have a passkey bound to the holder's account. A passkey is a public-key credential used through a browser, operating system or authenticator and may be unlocked by the holder's fingerprint, face recognition or device security mechanism. After successful ID PIN verification, the service shall require a fresh successful passkey assertion for the same holder, credential, session and requested operation. It

shall verify the challenge, authorized relying party and origin, credential binding, signature and required user-verification result under the W3C WebAuthn standard required by Title 2, Chapter 4, Article 15.

The Processor's authentication shall not satisfy the holder's requirement. The separate ID PIN remains required even where the passkey authenticator uses its own device-unlock PIN. A previous response shall not authorize a different session or operation.

Section 6: Current Validity and Restrictions

Before authorizing use, the service shall verify that the particular issuance is active, within its validity period and not suspended, revoked, replaced or disabled. It shall obtain current legal status and restrictions from the competent authoritative records and apply those relevant to the requested activity.

Each applied restriction shall identify its legal authority, scope and effective period. A restriction unrelated to the requested use shall not become a general denial of all uses. Static seal data shall not substitute for current status information.

Section 7: Verification Results

The result shall distinguish credential authenticity, holder authentication, current credential validity and permission for the requested use. A credential shall be accepted for that use only after every applicable condition is satisfied. A record lookup, visual preview or successful PIN check alone shall not constitute complete verification.

Service unavailability, unreadable features and unresolved discrepancies shall be recorded accurately and shall not be represented as successful verification. A capture failure alone shall not be recorded as a finding of forgery.

Section 8: Sessions and Audit

Each attempt shall have a unique session reference and a recorded purpose. The record shall identify the verifying person or service, credential issuance, time, profile version, stage outcomes, current status source, relevant restriction authority and final decision. Successful authentication shall be bound to its session and operation and expire under the prescribed session limits.

Section 9: Disclosure

The requesting service shall receive only the identity, status, result and restriction information necessary for its lawful purpose. Verification shall not disclose PINs, private keys, recovery material or unrelated protected particulars. An ID number search shall not itself authorize access to the complete identity record.

Section 8: Credential Lifecycle and Records

Title 2, Chapter 9 is amended by inserting Article 12 immediately after Article 11 as inserted by this Act and before Chapter 10, to read:

Article 12: Credential Lifecycle and Records

Section 1: Renewal and Replacement

The holder may apply for renewal or replacement through the Office. The Processor shall review current particulars, portrait and signature confirmation and required enrollment before issuing a new credential. Each issuance shall retain a distinct reference and status. The system shall prevent a superseded credential from inheriting the active status of its replacement.

Section 2: Loss and Compromise

The Office shall provide a means to report loss, theft or suspected compromise and record suspension of the affected credential or authenticator. The report, action, actor, time and reason shall be preserved. Reinstatement or replacement shall follow identity verification and the applicable review procedure.

Section 3: PIN and Passkey Recovery

Recovery shall verify the applicant's identity against the protected record and preserve the authorizing action. A reset shall replace the compromised secret or authenticator and invalidate the affected sessions. A Processor shall not retrieve an old PIN or substitute their own passkey for the holder's. The Ministry shall provide a recorded recovery procedure for loss of all enrolled authenticators.

Section 4: Decisions and Correction

Suspension, revocation, refusal and material corrections shall identify the competent authority, factual and legal basis, effective time and applicable review procedure. The holder may request correction of an administrative error and pursue administrative or judicial review according to law. Expiry and recorded authenticator failure shall not alter citizenship or the underlying competent refuge determination.

Section 5: Signature and Record History

The Office shall preserve issued particulars, credential and seal references, signature versions, approvals, corrections and status changes in an attributable history. A stored specimen signature shall not itself establish authorization of a later transaction. A signing service shall separately record the signed document or version, the holder's authorization, time and authentication event.

Section 6: System and Access Logs

Use of the registration and verification systems, record searches, protected-record access, exports, amendments, approvals, issuance, renewals, replacements and authenticator changes shall be logged automatically with the actor or service, time, purpose, affected record and outcome. Logs shall be protected against unauthorized alteration and access. Secret PIN contents, private keys and secret recovery material shall be excluded.

Section 7: Retention and Security

The Minister shall prescribe record-retention periods and requirements for preserving evidence needed for audit and lawful proceedings. Access controls, backups, incident handling, signing-key custody, key replacement and revocation, and the required technical preservation measures shall be implemented. The controls shall maintain record integrity and confidentiality through credential expiry and replacement.

Section 8: Electoral Secrecy

Identity verification records for an election shall be kept separate from ballot choices. General registration or verification logging shall not create a record linking the identified holder to the content of their secret ballot.

Section 9: Technical Requirements

The National ID issuing, trust and verification systems shall comply with Articles 8 through 12 and Title 2, Chapter 4, Article 17. Versioned technical specifications necessary to implement those requirements shall be published. The Office shall administer identity records, applications and registration decisions. The standards shall define supported media, reader capabilities, interfaces, conformance tests and deployment requirements. A profile shall be accepted only after its required functions have been demonstrated.

Section 10: Continuous Person and Credential History

Every person shall have a permanent registry-person reference independent of any online account, credential class or integration tier. All credentials previously issued to that person shall be retained under that reference, including credentials issued before the person created an online account.

Upon verified linking of an account, the system shall automatically retrieve and associate the person's existing registry and credential history with the account's authorized identity view. Issuing an account-linked credential shall continue that history rather than create a new person record. Existing National ID numbers, aliases of historical identifier schemes and prior credential references shall remain traceable to the permanent record.

Section 11: History View and Status Transitions

The internal identity view shall provide a chronological history showing each issuance reference, National ID number used, class, integration tier, recorded legal status, issue and expiry dates, issuer, status changes and the reason and authority for replacement, renewal or transition. Each entry shall link to its immutable issuance snapshot, seal reference and predecessor or successor credential where applicable. Earlier entries shall retain the particulars applicable at that time.

A change from non-account to account-linked status, from refugee to citizen status, or between credential classes shall be recorded as a dated transition with its supporting authority. The account, current person record and new credential shall show the current effective status; historical records shall show the former status. A change of status shall not reactivate superseded credentials or remove an independently continuing lawful restriction.

The system shall enforce access according to the requesting person's function and lawful purpose. Historical refugee status or other former particulars shall not be disclosed to a routine verification requester merely because that requester is entitled to verify the current credential.

Section 12: Verified Linking and Duplicate Records

Before linking historical records, the Processor shall establish continuity of identity through the existing National ID and its applicable NCVS checks or a recorded identity-recovery procedure, and confirm control of the account to be linked. A match based solely on a name, resemblance or newly supplied account details shall not authorize a merge. Possible duplicate records shall be referred for review.

An authorized civil-registration decision may reconcile duplicate records after supporting evidence is examined. The reconciliation shall preserve former references, issuance snapshots and events and record the deciding person, evidence, reason and time. An incorrect link shall be reversible through a recorded correction without destroying the original histories. Account deletion or unlinking shall preserve the civil-registration history required by the applicable retention rules.

Section 9: Electoral and Parliamentary Identification

Title 2, Chapter 10, Article 2 is amended by inserting Section 8 immediately after Section 7, to read:

Section 8: National ID Verification for Candidacy and Parliamentary Office

Every candidate for an elected parliamentary seat, Chancellor or Vice Chancellor must hold an active National ID before their candidacy is accepted. Each member of a joint ticket shall satisfy the requirement individually. Nomination, ballot identification and certification shall use the legal name recorded in the Civil Registry. Additional registered name components may be included in accordance with Title 2, Chapter 9, Article 8, Section 5.

The National Electoral Administration shall verify identity, active credential status and electoral eligibility against the competent records. A person automatically nominated for reelection shall be verified before certification. An applicant shall have a reasonable opportunity to correct a registry or identification error before the applicable nomination deadline, but shall not be certified while a required qualification remains unsatisfied.

Every person elected, returned unopposed or appointed to either House, including the Vice Chancellor taking a seat by virtue of office, must hold an active National ID verified before assuming parliamentary office. The competent parliamentary authority shall record compliance without publishing confidential identifiers. A sitting member shall maintain an active National ID; later identification deficiencies shall be referred for correction and handled under constitutional rules governing removal, recall and vacancies.

Authentication of an application through a digital service shall comply with NCVS. Verification of identity shall remain separate from determination of citizenship and other electoral qualifications.

Section 10: Firearms Identification

Title 7, Chapter 9, Article 3, Section 2 is amended to read:

Section 2: Required Registration Information

A person acquiring or possessing a civilian firearm shall register the firearm by providing ~~the registrant's lawful identity~~ the registrant's legal name and active National ID verified through the Civil Registry; a reasonable description of the firearm; any serial number, unique identifier, or identifying mark where one exists; the means by which the firearm was acquired; and any additional information specifically required by a Policy Order reasonably necessary to identify the firearm and lawful possessor.

Title 7, Chapter 9, Article 3 is amended by inserting Section 9 immediately after Section 8, to read:

Section 9: Active National ID Requirement

A person acquiring or possessing a civilian firearm must hold an active National ID. The firearms-registration authority shall verify the credential and any applicable restrictions against the competent records. This requirement shall be subject to the public referendum required by Section 12 of the National ID Act of 2026.

Section 11: Security Standards for Official Digital Services

Title 2, Chapter 4 of the Civil Code is amended by inserting Article 17 immediately after Article 16, Doctrine of Functional Delegation, as inserted by the Chancellery and Imperial Household Administration Expansion Act of 2026, and before Chapter 5, to read:

Article 17: Security of Official Digital Services

Section 1: Covered Services

Every digital service operated by or on behalf of a state organ shall comply with this Article. Coverage includes public websites, authenticated services, internal applications, interfaces, identity providers, administrative tools and the supporting systems through which their security or protected records may be affected. The same requirements shall apply where a service is procured, externally hosted or operated by a contractor.

Section 2: Critical Services

Every page, application, function and interface provided at totemiaempire.com or parliament.totemiaempire.com shall be a critical digital service. Its classification shall apply to public and restricted areas alike. An identity provider, database, administrative interface or other supporting system capable of controlling the service or exposing or altering its protected records shall be included in its critical security boundary, even when hosted elsewhere.

The Emperor may designate additional critical services by Imperial Order. An inventory of covered services and their dependencies shall be maintained.

Section 3: Application Security Standard

Every covered service, including a service not classified as critical, shall meet all applicable Level 1, Level 2 and Level 3 requirements of the OWASP Application Security Verification Standard (ASVS), version 5.0.0, subject only to the temporary hardware-authenticator exception in Section 8.

The implementation record shall identify each requirement by its versioned identifier, its implementation and the evidence used to verify it. A requirement may be recorded as inapplicable only where the relevant function or technology is absent and the recorded reason establishes that the security objective is unaffected. Cost, inconvenience or a failed implementation shall not make an applicable requirement inapplicable.

Section 4: Critical Authentication and Passkeys

Human authentication to protected functions of every critical service shall meet the applicable technical requirements of NIST Special Publication 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, published in July 2025. Ordinary account access shall meet

Authentication Assurance Level 2 and shall use phishing-resistant passkey authentication with user verification. Privileged access that can issue credentials, alter identity or legal-status records, administer accounts, change security settings or control deployment shall meet Authentication Assurance Level 3, subject to Section 8.

Passkey registration and authentication shall comply with the relying-party requirements of W3C Web Authentication: An API for accessing Public Key Credentials, Level 3, Recommendation of August 25th, 2026. The service shall verify a fresh unpredictable challenge, the authorized origin and relying-party identifier, the registered credential, the signature, user presence and required user verification. A successful response shall be bound to the intended account and session. The service shall prevent reuse for another authentication operation.

Public information may remain accessible without authentication. Machine and service accounts shall use separately authenticated, restricted cryptographic credentials under the applicable ASVS controls; they shall not share a person's passkey or acquire human privileges through an unauthenticated interface.

Section 5: National ID PINs and Protected Functions

The holder PIN required by Title 2, Chapter 9, Article 11 shall remain a separate verification condition. A National ID number, static card image, signed seal or holder PIN shall not by itself satisfy the authentication required for protected access under Section 4. A static card or seal shall not be counted as proof that the holder controls a cryptographic authenticator.

A holder of a non-account credential may use an authorized Processor for a function for which that form of credential is permitted. The Processor shall authenticate through the applicable protected service, verify the holder under NCVS, and record the act in the holder's proper capacity. The holder PIN shall not authorize remote access to the protected account or records, substitute for the Processor's authentication or be represented as establishing a NIST assurance level by itself.

Section 6: Secrets and Identity Records

Stored identity particulars, portraits, signatures, credential histories and backups shall be protected by the applicable ASVS cryptographic, data-protection and access-control requirements. Encryption keys and signing keys shall be managed separately from the records they protect. Authorization shall be enforced by the service for each protected operation, and access and material changes shall be recorded.

A centrally verified holder PIN shall be stored only as a uniquely salted, computationally costly one-way verifier with additional secret protection held separately from the verifier database. PINs, private authentication keys and recovery secrets shall be excluded from ordinary records, telemetry and logs. Passkey private keys and biometric samples shall not be collected by the relying party as part of passkey registration or verification.

Section 7: Implementation and Maintenance

Covered services shall be designed, implemented, tested, operated and maintained in accordance with this Article. Security controls, maintenance, incident response and compliance evidence shall be documented.

Section 8: Temporary Hardware-Authenticator Exception

Until an HACD under Section 9 takes effect for the stated service and users, compliance with this Article may use synchronized browser, operating-system or phone passkeys meeting the applicable AAL2 requirements. The mandatory use of a hardware-protected, device-bound authenticator with a non-exportable private key, and the dependent client-authenticator requirements necessary to attain AAL3 or the ASVS Level 3 hardware requirement, shall be deferred for those users.

The exception is confined to those hardware-dependent requirements. Multi-factor authentication, required passkeys and user verification, phishing and replay resistance, protected communications, secure recovery, secret storage, server-side cryptographic protection and all other applicable requirements shall remain mandatory. Privileged critical access during the exception shall meet AAL2 with mandatory phishing-resistant passkeys, restricted permissions, security logging and renewed authentication for sensitive operations.

The deferred requirements, resulting risks and mitigating controls shall be documented. The deployment shall be described as operating under this statutory hardware exception. Full AAL3 or unqualified ASVS Level 3 conformity shall not be claimed while a required control remains deferred.

A qualifying hardware authenticator may be built into a device or be an external security key. It need not be manufactured or issued by the Totemian Government. A compatible device alone shall not end the exception before the required HACD takes effect.

Section 9: Activation with Imperial Approval

A Hardware Authentication Commencement Declaration (HACD) may be issued under lawful authority after verification that compatible authenticators, enrollment, replacement, recovery, technical support and the required conformance evidence are available for the stated users. The HACD shall identify the service, covered users or account classes, applicable requirements, evidence of readiness, migration arrangements and prospective effective date.

The HACD must be signed under lawful authority and receive the Emperor's express signed approval before taking effect. Imperial assent to the Act establishing this Article shall not itself constitute approval of a later HACD. The approved HACD and effective date shall be communicated to affected users before the requirement takes effect; confidential security evidence may be retained separately.

From that date, the identified hardware requirements shall apply to the stated service and users, including AAL3 where Section 4 requires it. Users shall have a conforming enrollment and recovery route before their access is made dependent upon the activated requirement. An activated requirement shall not be waived without further authority in law or an Imperial Order.

Section 10: Verification and Versions

A documented security assessment by a suitably qualified reviewer shall be completed before production deployment and after a material change to authentication, authorization, sensitive-data handling or the security boundary. The assessment shall identify the tested version, applicable requirements, deferred hardware controls, findings and corrective work. An applicable failed control shall be corrected before the affected new or changed protected function enters production.

The standard versions named in this Article shall remain controlling until amended by law or an Imperial Order specifying the replacement version and migration arrangements. The incorporated provisions govern technical security; they shall not adopt foreign institutions or foreign governmental procedures as Totemian law.

Procurement and maintenance arrangements shall require the evidence and continuing controls necessary for compliance.

Section 12: Public Approval of the Firearms Requirement

Following Imperial assent, the National Electoral Administration shall submit the amendments in Section 10 to a public referendum without requiring a petition or further parliamentary referral. The referendum shall open on November 14th, 2026 and close on November 16th, 2026, with voting available for at least 48 continuous hours, provided the measure is qualified by October 31st, 2026 and the required proclamation and advance publication are completed under Article 20, Section 16 of the Constitution. If those conditions are not met, the National Electoral Administration shall conduct the referendum on the earliest lawful dates fixed under that Section, maintaining the required notice and voting period. Approval shall require at least 60% of the valid votes cast in favor of or against the question. The restrictions in Section 10 shall not apply before certification of referendum approval.

The National Electoral Administration shall assign a proposition number and publish the following ballot wording with that number inserted:

PROPOSITION [number]

Referred to the People of the Totemian Empire by the Parliament of the Totemian Empire

RELATING TO CIVILIAN FIREARM IDENTIFICATION

OFFICIAL TITLE

AMENDING TITLE 7, CHAPTER 9, ARTICLE 3, SECTION 2 OF THE CIVIL CODE; ADDING SECTION 9 TO THAT ARTICLE; RELATING TO CIVILIAN FIREARM IDENTIFICATION.

DESCRIPTIVE TITLE

REQUIRES AN ACTIVE NATIONAL ID TO ACQUIRE OR POSSESS A CIVILIAN FIREARM AND VERIFICATION THROUGH THE CIVIL REGISTRY FOR FIREARMS REGISTRATION.

A vote IN FAVOR shall have the effect of amending civilian firearm registration law to require a person to hold an active National ID to acquire or possess a civilian firearm and to have that ID verified through the Civil Registry.

A vote AGAINST shall have the effect of retaining existing law relating to the identification and registration of civilian firearm holders, without introducing this active National ID requirement.

Select 1 choice

IN FAVOR

AGAINST

APPROVAL AND LEGAL EFFECT

Approval requires at least 60% of the valid votes cast IN FAVOR or AGAINST. The requirement takes effect only after approval is certified.

Notice: A law approved by public referendum may not be amended, repealed, suspended, or weakened by Parliament for 90 days after certification unless the change is approved by another public referendum.