



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Government & Public Services**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Information System Authority · Police and Border Guard Board · Data Protection Inspectorate**

Key takeaways

- Estonia's public sector identifies people online through state electronic identity (eID): the ID card, the residence permit card and Mobile-ID, all notified to the EU at the highest assurance level ("high"), plus the privately run Smart-ID, which Estonia's Information System Authority rates "high" nationally.
- Government bodies are not covered by Estonia's anti-money laundering (AML) law. Identity in the public sector is governed by the identity document rules and the EU electronic identification regulation (eIDAS), not by customer due diligence rules.
- Online and in-person routes differ sharply: an ID card renewal can be applied for entirely online, but a first identity card, fresh fingerprints and the collection of every card still require a physical visit.
- Public e-services must accept EU Digital Identity Wallets from the end of 2026, and some regulated private services from the end of 2027. Estonia's own wallet was still at the procurement stage in mid-2026.
- A bill, not yet law, would move e-residents to remote biometric identity checks from March 2027 and to a cardless eID from March 2028.

Estonia is open to digital public services by default: most state services are reached online with a national eID through a single state login platform run by the Information System Authority (RIA). The Police and Border Guard Board (PBGB) issues the identity documents that carry the eID and operates the notified eID scheme.

For a provider building public-sector or eID-dependent services, the main constraint is not a licence but the credential itself: every Estonian eID is rooted in an in-person, biometric enrolment, and the rules on which credentials a service may accept, and how, are set by RIA's platform terms and by eIDAS.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Authority	Remit in public-sector identity	Level	Official site
Information System Authority (Riigi Infosüsteemi Amet, RIA)	eID strategy, quality and security requirements for eID, ID software, the State Authentication Service (TARA) and State SSO (GovSSO), EU Digital Identity Wallet procurement and relying-party register	National	ria.ee
Police and Border Guard Board (Politsei- ja Piirivalveamet, PBGB)	Issues ID cards, residence permit cards and e-resident digital IDs; authority responsible for the notified Estonian eID scheme	National	politsei.ee
Ministry of Justice and Digital Affairs	Legislation on the security requirements of public key infrastructure (PKI) services	National	justdigi.ee
Ministry of Foreign Affairs	Issues diplomatic identity cards; Estonian embassies receive and hand over documents abroad	National	vm.ee
Data Protection Inspectorate (Andmekaitse Inspektsioon)	Supervises the processing of personal data, including identity and biometric data	National	aki.ee

European
Commission

Publishes the list of notified eID
schemes and the implementing acts
for EU Digital Identity Wallets

Supranational

[eur-
lex.europa.eu](https://eur-lex.europa.eu)

The Ministry of the Interior sets, by regulation, the list of nationalities whose e-resident applications are restricted, and the Estonian Business and Innovation Agency runs the e-Residency programme; neither is a supervisory authority for identity verification.

2

Licensing and authorisation

No licence is needed to build a service that relies on Estonian eID, but access to the state's authentication infrastructure is restricted and contractual.

State authentication platforms

RIA provides TARA and GovSSO only to government-sector authorities listed in the Ministry of Finance classification of public sector institutions, excluding the "other public sector" category. An institution applies with a digitally signed application, must complete integration with the demo service before production, and joins on terms and forms valid from 1 March 2025 ([RIA, Authentication services](#)). Private providers integrate with the eID methods directly or through a commercial broker rather than through TARA.

Private eID schemes

Smart-ID is provided by SK ID Solutions AS, a private company. Before it was accepted in state e-services, an expert group convened by RIA, with the PBGB, the Ministry of the Interior and the Ministry of Economic Affairs and Communications, assessed its assurance level as "high" for persons with an Estonian personal identification code ([RIA, Electronic identity](#)). Smart-ID is not on the European Commission's list of notified eID schemes.

Relying on EU Digital Identity Wallets

Under Regulation (EU) 2024/1183, relying parties that intend to use wallets register in the Member State where they are established; recital 17 states that registration should be proportionate, automated where possible and should not entail a pre-authorisation process ([Regulation \(EU\) 2024/1183](#)). RIA plans the minimum viable version of Estonia's relying-party register for the end of 2026 or early 2027, with registration opening afterwards Planned, end 2026 / early 2027 ([RIA, EUDI Wallet](#)).

Identity framework (AML rules do not apply)

Public authorities acting in their public capacity are not obliged entities. Section 2 of the Money Laundering and Terrorist Financing Prevention Act (Rahapesu ja terrorismi rahastamise tõkestamise seadus) lists credit and financial institutions, gambling operators, traders above cash thresholds, legal professionals and others, but not government bodies; section 34 instead lists a governmental authority, or a body performing public functions in Estonia or the European Economic Area, as a lower-risk customer for obliged entities ([Money Laundering and Terrorist Financing Prevention Act, version in force from 21 July 2026](#)).

Identity in the public sector rests on three layers instead:

Identity documents

The ID card is the primary eID carrier and is compulsory under Estonian law; the residence permit card plays the same role for non-EU foreigners. Documents are issued by the PBGB under the Identity Documents Act ([RIA](#)).

Notified eID scheme

The Estonian eID scheme (ID card, residence permit card, Digi-ID, e-Residency Digi-ID, Mobile-ID and diplomatic identity card) is notified under Article 9 of eIDAS at level high, with the PBGB as the responsible authority ([C/2024/7543](#)).

eIDAS and the wallet framework

Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, governs cross-border recognition, trust services and EU Digital Identity Wallets.

Where the public eID is used by a regulated private firm, the AML Act sets the bar: for remote due diligence, credit and financial institutions may use an eID scheme notified at level substantial or high, or a qualified trust service (section 31(3)); if an e-resident's digital ID is used remotely, another identity document must be used at the same time (section 31(4)); and they may use personal identification data from the identity documents database (section 31(5)).

How the state enrolls a person

A first ID card requires proof of Estonian citizenship, presented with an identity document at a PBGB client service office. Fingerprints remain valid for six years; people over 70 who have already given fingerprints need not give them again ([PBGB, Application at a client service office](#)). A document photograph, fingerprints and specimen signature taken in a PBGB service office photo booth can be reused in an online application for up to 183 days ([PBGB, self-service application](#)). Collection is physical: the applicant presents the existing ID card (or a person authorised at the time of application collects it with their own Estonian identity document), and a card can be collected in a partner shop only if the applicant brings a valid PBGB-issued document ([PBGB, Collection](#)).

Derived credentials

Mobile-ID keys sit on a special SIM card, and an ID card is needed to apply for it. Smart-ID can be issued only to persons with an Estonian personal identification code. RIA reports about 1.2 million valid ID cards and 219,000 Mobile-ID users (July 2026). Digital ID, a card for electronic use only, stopped being issued to Estonian residents on 1 May 2025; cards issued earlier remain valid until expiry ([RIA, Electronic identity](#)).

Authenticating users of a public e-service

TARA lets an institution offer the ID card, Mobile-ID, Smart-ID and EU eIDs separately or together; GovSSO adds a single sign-on session. Mobile-ID and Smart-ID in GovSSO are available only to users with an Estonian personal identification code. Public e-services must support another Member State's notified eID within one year of the Commission's implementing decision on that scheme ([RIA, Authentication services](#)).

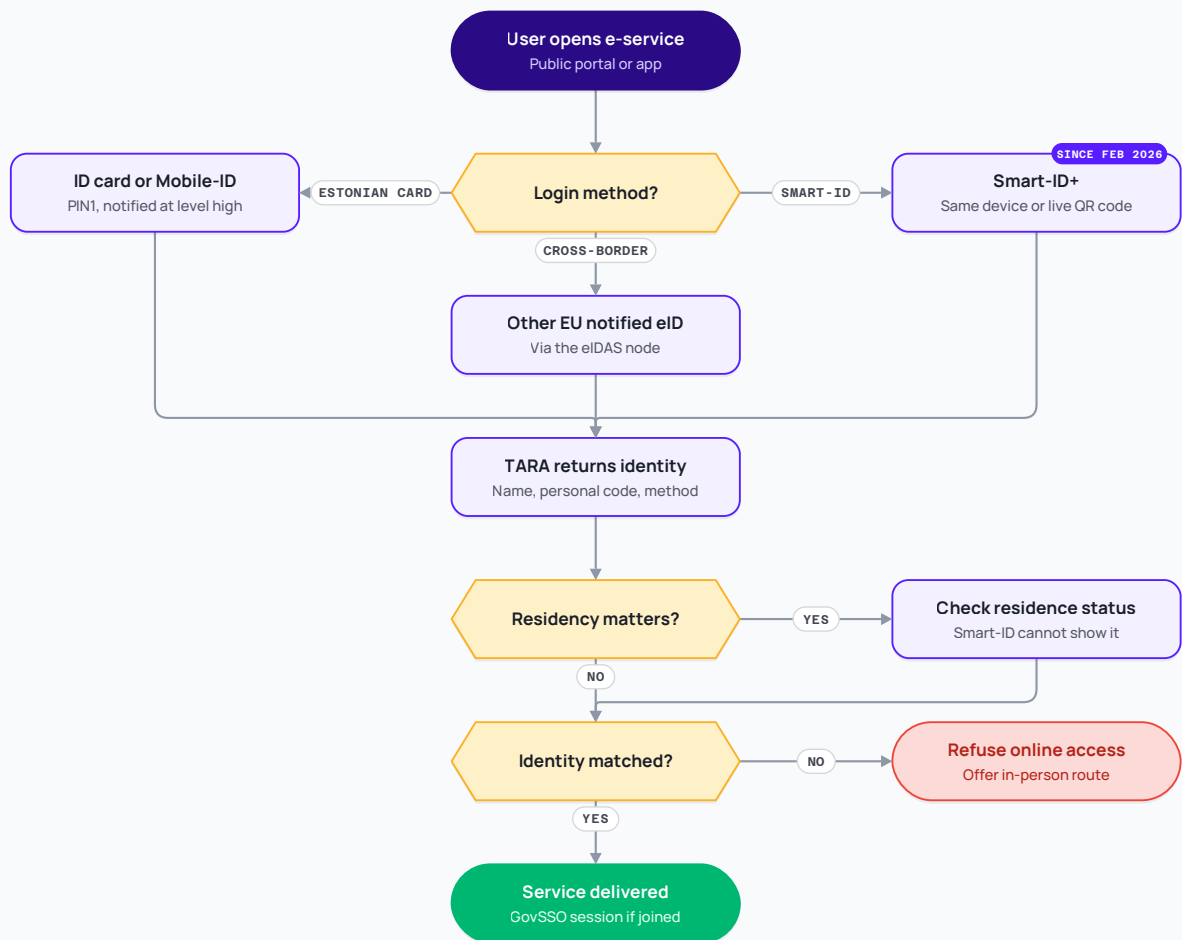


Figure 1. Signing in to an Estonian public e-service through the State Authentication Service (TARA).

5 Digital channels: what's different

Bottom line: almost every public service is online, but the online channel depends on a credential that is always enrolled and collected in person; no route currently issues a first Estonian eID entirely remotely.

Requirement	In person	Online / remote	Difference
First ID card	Client service office, proof of citizenship	Not available	Differs
ID card renewal	PBGB office	Self-service portal with ID card, Mobile-ID or internet bank login	Differs

Biometrics	Captured at the office	Reused if fingerprints are under six years old or booth captures under 183 days	Differs
State fee, adult ID card	€45	€35	Differs
Collecting the card	Holder or authorised person, in person	Same: physical collection at an office or partner shop	Same
e-Resident application	Not accepted	Online only, submitted by the applicant, no intermediaries	Differs
e-Resident card collection	In person, fingerprinted, foreign travel document	No remote option	Same
Proof of residence status	Shown by the document	Not distinguishable with Smart-ID	Differs

Sources for the table: [PBGB self-service](#) (fees from 1 January 2025), [PBGB office application](#), [PBGB collection](#), [PBGB e-resident FAQ](#), [RIA](#).

Smart-ID+ ends remotely initiated logins

Since 26 February 2026, TARA and GovSSO use Smart-ID+: on a phone the user opens the app directly, and on a computer the user scans a continuously changing QR code. A login can no longer be initiated remotely; the devices must be the same or physically close, which RIA describes as a measure against social engineering fraud ([RIA, Accessing state e-services with Smart-ID](#)). Private services relying on Smart-ID should expect the same pattern.

E-residents: online application, physical issue

An e-resident's digital ID lets a foreign national without Estonian residence identify themselves and sign electronically; it confers no right of residence. The applicant must fill in and submit the application personally in the PBGB environment; the PBGB may hold a video interview where needed, decides within 30 days, and issues the card only in person, with fingerprinting, at a PBGB office, embassy or mobile pick-up point ([PBGB, e-resident FAQ](#); [PBGB, Pick-up](#)).

Pending changes

Bill 905 SE **Bill, first reading passed 1 Jun 2026** would introduce remote verification of e-residents' identity using biometric data and travel-document data from March 2027 and a cardless e-resident eID from March 2028 ([Riigikogu](#)). The draft requires that the integrity and authenticity of the data on the foreign biometric passport chip can be verified throughout the right's validity ([Bill 905 SE, draft section 34⁶](#)).

6

Data protection and biometrics

The General Data Protection Regulation (Regulation (EU) 2016/679) applies to all identity data processing, and eIDAS is expressly without prejudice to it (Article 2(4) of Regulation (EU) No 910/2014 as amended). The state's own biometric holdings are long-lived: according to the PBGB, data submitted with an e-resident application are kept in the identity documents database for 75 years, while facial images and fingerprints are stored in the automated biometric identification system (ABIS), actively for 15 years and then in an archive for 60 years, and deletion cannot be requested after an application is submitted ([PBGB, e-resident FAQ](#)).

For services accepting EU Digital Identity Wallets, the wallet must give users a dashboard to see every relying party, request erasure of their data and report a relying party to the data protection authority (Article 5a(4)(d)). Recital 17 expects relying parties to carry out data protection impact assessments where processing is high-risk, and recital 32 bars wallet providers from seeing users' transactions ([Regulation \(EU\) 2024/1183](#)). In Estonia the Data Protection Inspectorate is the competent authority for such reports.

7

Sector-specific obligations

Accept EU Digital Identity Wallets

Each Member State must provide at least one wallet within 24 months of the entry into force of the implementing acts, and wallets must meet assurance level high (Article 5a(1) and 5a(5)(d), [Regulation \(EU\) 2024/1183](#)). RIA states that the first implementing acts entered into force on 24 December 2024, so public-sector e-services that require electronic identification must accept wallets from the end of 2026 **Applies end of 2026**, extending to certain regulated private services from the end of 2027 **Applies end of 2027**. Estonia's own wallet tender was launched on 18 May 2026, with roughly a year expected to

award the contract ([RIA, EUDI Wallet](#)), so Estonian services may first meet other countries' wallets.

Support the new ID card platform

Thales took over ID card production from IDEMIA in November 2025, and Zetes became a qualified trust service provider on 20 October 2025 for the new cards' certificates. RIA told service providers to support both trust service providers, including Zetes's certificate chain and OCSP validity service; without the updates, new cards cannot be used electronically in their systems ([RIA, 30 October 2025](#)).

E-residency eligibility controls

Since 1 October 2025, applications from citizens of ten listed countries (including Iran, Nigeria and Syria) are reviewed only if, for example, the applicant has lived in the EEA, the United Kingdom or Switzerland for three consecutive years with a valid permit, or has permanent economic activity in Estonia. Applications from Russian and Belarusian citizens are reviewed only if the applicant previously held an e-resident digital ID and has permanent economic activity in Estonia ([PBGB, Citizenship-based restrictions](#)).

Risk indicators and red flags

IDENTITY-ABUSE INDICATORS FROM OFFICIAL SOURCES

- **Remotely initiated login:** a PIN request the user did not start, the pattern Smart-ID+ was introduced to stop.
- **Intermediary-submitted e-resident applications:** the PBGB does not accept applications filled in or submitted by agents.
- **Resident status assumed from Smart-ID:** Smart-ID does not distinguish residents from non-residents.
- **Unexplained purpose:** e-resident applicants who cannot show how use of the ID contributes to Estonia's economy, science, education or culture.
- **Restricted nationality without exception:** applications from listed countries lacking residence or economic-activity evidence.
- **Doubtful true identity:** the PBGB may require a video interview or a personal visit before issuing.
- **Outdated certificate validation:** systems that do not check Zetes's OCSP service for cards issued from November 2025.

Enforcement and penalties

Public-sector identity rules are enforced chiefly through administrative measures rather than fines. The PBGB can dismiss an application when requested information is not provided, refuse issue, and revoke an e-resident's digital ID; the state fee is not refunded when an application is refused or a document is revoked. When an e-resident's digital ID ceases to be valid, a Smart-ID account created with it is closed, under the agreement between Estonia and SK ID Solutions ([PBGB, e-resident FAQ](#)).

For obliged entities that rely on eID, the AML Act treats a relationship established without physical presence, where the section 31 safeguards are not applied, as a higher-risk factor (section 37(3)(4)), and requires enhanced due diligence where there are doubts about the authenticity of documents or the truthfulness of submitted data (section 36(2)(1)) ([Money Laundering and Terrorist Financing Prevention Act](#)).

10 Recent changes and what to watch

- **End of 2026 and 2027** **Applies end of 2026 / 2027** : public e-services must accept EU Digital Identity Wallets, followed by certain regulated private services. Plan wallet acceptance and relying-party registration now.
- **1 June 2026** **Bill, first reading passed** : Bill 905 SE on remote, cardless e-residency. Remote biometric proofing of foreigners would become part of the state model from March 2027 if enacted.
- **18 May 2026** **Procurement launched** : RIA's international tender for the Estonian EU Digital Identity Wallet. A contract is expected about a year later.
- **26 February 2026** **In force** : Smart-ID+ in TARA and GovSSO. Same-device links and live QR codes replace remotely initiated logins.
- **November 2025** **In force** : Thales-produced ID cards with Zetes certificates. Relying parties must validate two trust service providers.
- **1 October 2025** **In force** : nationality-based restrictions on e-resident applications. Expect fewer new e-residents from listed countries.
- **1 May 2025** **In force** : Digital ID no longer issued to residents. Existing cards run to expiry.

11 What this means for identity verification

For users with an Estonian personal identification code, the ID card and Mobile-ID provide a notified level-high credential, and Smart-ID a nationally rated one; document capture is rarely needed for them. Foreign users fall into two groups: EU citizens with a notified eID from another Member State, who can be accepted through the eIDAS node, and e-residents, whose card proves identity electronically but not residence, and who for AML purposes must be paired with a second document.

Services must handle the full set of live document generations, including cards issued from November 2025 under a new trust service provider, and must not infer residence from a Smart-ID login. Where onboarding is remote and no notified eID is available, document verification with NFC chip reading of a biometric passport, face match and liveness detection is the route the e-residency reform itself proposes. Retention design should reflect that identity evidence held by the state is retained for decades, whereas relying parties remain bound by data minimisation. Re-verification triggers include card replacement, certificate revocation, expiry of an e-resident ID and the arrival of wallet-based credentials from the end of 2026.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- ID document capture and verification, including NFC chip reading of biometric passports, for users without an Estonian eID.
- Face match and biometric liveness detection for remote onboarding where no notified eID is available.
- No-code workflow builder to route users between national eID login and document-based verification.
- Cloud, on-premises or hybrid deployment to fit public-sector hosting and data residency requirements.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Electronic identity (eID)**, Information System Authority, last updated 20 July 2026, ria.ee
- **Authentication services (TARA and GovSSO)**, Information System Authority, last updated 17 July 2026, ria.ee
- **Accessing state e-services with Smart-ID**, Information System Authority, last updated 7 March 2026, ria.ee
- **EU Digital Identity Wallet**, Information System Authority, last updated 22 July 2026, ria.ee
- **RIA: service providers need to prepare their IT systems for the arrival of new ID cards**, Information System Authority, 30 October 2025, ria.ee
- **Applying for an ID card for an adult: self-service portal; client service office; Collection**, Police and Border Guard Board, politsei.ee, politsei.ee, politsei.ee

- E-Resident's digital ID: What is it; Pick-up; Frequently asked questions; Citizenship-based application restrictions, Police and Border Guard Board, politsei.ee, politsei.ee, politsei.ee, politsei.ee
- Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act], sections 2, 31, 34, 36 and 37, version in force from 21 July 2026, Riigi Teataja, riigiteataja.ee
- Isikut tõendavate dokumentide seaduse muutmise ja sellega seondult teiste seaduste muutmise seadus [Bill 905 SE amending the Identity Documents Act], initiated by the Government on 7 May 2026, Riigikogu, riigikogu.ee
- A bill specifying e-residency passed its first reading in the Riigikogu, Riigikogu, 1 June 2026, riigikogu.ee
- Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 30 April 2024, Articles 2(4), 5a(1), 5a(4) (d), 5a(5) (d) and recitals 17 and 32, eur-lex.europa.eu
- Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014, C/2024/7543, OJ C, 20 December 2024, eur-lex.europa.eu