



State Comptroller  
of Israel

---

# Authentication of Public Documents at the Ministry of Foreign Affairs – Apostille

---

▪ February 2026 ▪



---

# Authentication of Public Documents at the Ministry of Foreign Affairs – Apostille

## Abstract

### Background

In order to simplify the process of authenticating public documents between countries, the Apostille Convention was signed in The Hague on October 5, 1961. The apostille serves as a certificate of authenticity that ensures the reliability of public documents (such as a birth certificate, marriage certificate, criminal record certificate, academic certificate, medical certificate, and others), and provides the legal confirmation required for them to be recognized as valid and acceptable in all countries that are parties to the Convention.

For the purpose of implementing the Convention, the Apostille Convention Implementation Regulations<sup>1</sup> were enacted in 1977, constituting the implementing provisions of the Convention in Israel. Under these regulations, the Ministry of Foreign Affairs and a registrar of a Magistrate's Court, or a civil servant appointed by the Minister of Justice, were designated as the competent authorities to issue apostille certificates. In 2020, following a government decision<sup>2</sup> to allow the issuance of digital apostilles by all government ministries and public authorities, the Director of the Notary Licensing Department at the Ministry of Justice was authorized as the competent authority to sign digital apostilles. At the Ministry of Foreign Affairs, the Public Documents Authentication Unit, operating within the Consular Division, is responsible for authenticating public documents, whether under the Apostille Convention or for countries that are not parties to the Convention<sup>3</sup>. The Ministry of Foreign Affairs authenticates dozens of types of public documents issued by approximately 60 government ministries and public bodies.

The competent authority issuing apostille certificates has three main functions<sup>4</sup>: (a) to verify the authenticity of public documents; (b) to issue apostilles; and (c) to maintain a register of the details of apostille certificates issued, enabling any interested party – including the destination country – to verify the apostille.

---

1 Regulations for the Implementation of the Hague Convention (Abolishing the Requirement of Legalisation for Foreign Public Documents), 5737-1977.

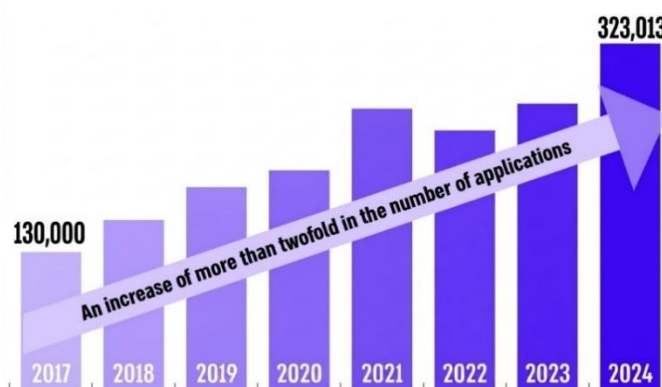
2 Government Decision No. 260, "Plan to Accelerate Digital Services to the Public and Promote Digital Learning" (July 26, 2020), Sections 25–27.

3 Authentication of public certificates for destination countries that are not parties to the Apostille Convention; for example, Ethiopia.

4 See paragraph 40 on p. 37 of the practical handbook for the implementation of the Convention, and the section "Role of authorities" in the document outlining the Convention's key principles at the following link: <https://assets.hcch.net/docs/80d0e86f-7da8-46f8-8164-df046285bcdd.pdf>.

The Hague Conference on Private International Law (HCCH)<sup>5</sup> has published a practical handbook<sup>6</sup> for the implementation of the Convention. The handbook details the process for authenticating signatures: a competent authority in the country that issued the original document examines the document and verifies the authenticity of the signature, seal, or authorized signatory appearing on it. Upon completion of the authentication process, the authority issues the apostille, which serves as confirmation of the authentication and forms an integral part of the original document when it is presented. The original document, together with the apostille, is recognized without the need for additional authentication or legalization<sup>7</sup> in all countries that are parties to the Convention. This procedure ensures uniformity, reliability, and efficiency in international document authentication processes.

### Growth in the Demand for Authentication of Public Documents, 2017–2024



Based on data from the Ministry of Foreign Affairs, processed by the State Comptroller's Office.

- 5 The Hague Conference on Private International Law (HCCH) is an intergovernmental organization whose purpose is the progressive unification of the rules of private international law. The organization drafted the Apostille Convention and continues to promote it, oversee its implementation, provide guidance on its proper application, and update and improve it in accordance with the evolving needs of the international community. For information about the organization, see: <https://www.hcch.net/en/about>.
- 6 Apostille Handbook – Practical Handbook on the Operation of the Apostille Convention <https://assets.hcch.net/docs/a19ae90b-27bf-4596-b5ee-0140858abeaa.pdf>.
- 7 Treaty Series 855, Vol. 25 – Convention Abolishing the Requirement of Legalisation for Foreign Public Documents (5739-1979), Article 2.

## Key Figures

854,000

apostille certificates were issued by the Ministry of Foreign Affairs in the years 2022–2024; in 2024 alone, 323,000 certificates were issued

77%

of all apostille certificates were issued without verification of signatures<sup>8</sup> as required under the Apostille Convention

51%

Share of authorized signatories whose records in the authentication system lack essential information, such as a specimen signature, without which the document signatory cannot be properly verified

Only 0.8%

Share of digital apostille certificates issued (7,100) out of the total certificates issued (854,000) in the years 2022–2024

80%

Rate of decline in the number of appointment slots allocated monthly by the Ministry of Foreign Affairs in the years 2023–2024 for in-person document authentication services

0.007% (167)

Share of all apostille fee purchasers who accounted for **62% of all fees** paid in 2023, **totaling NIS 4,700,000**

NIS 50 million

Minimum amount paid by citizens for courier services in 2023 alone (based on an average price quotation of NIS 400 per document)

0

Shaded seating areas, restroom facilities, and water stations available for the public waiting for hours outside the gates of the Ministry of Foreign Affairs

38

Days of telephone service during which none of the incoming calls were answered; in total, **4,499 callers waited on the line in vain**

9.2%

of the receipts (6,542 out of 71,173) in the authentication system do not match the receipt data in the government payment system

65%

of the receipts in the authentication system at the Ministry of Foreign Affairs were recorded with fee amounts lower than those prescribed in the regulations

36%

of the self-service digital kiosks for government services that were examined were found to be malfunctioning

<sup>8</sup> The system does not contain the signatures of authorized signatories, the seals of the relevant public bodies, or the characteristics of the security features.

---

## Audit Actions



From June 2024 to March 2025, the State Comptroller's Office examined the implementation of the Apostille Convention at the Ministry of Foreign Affairs. As part of the audit, databases of the Ministry of Foreign Affairs and the National Digital Agency were analyzed, and overt and covert observations and inspections were conducted in the Official Passports and Official Visas Department of the Consular Affairs Division at the Ministry of Foreign Affairs. The audit was conducted at the Ministry of Foreign Affairs; supplementary examinations were carried out at the Ministry of Justice, the National Digital Agency, and the Population and Immigration Authority (Population Authority). Among other matters, the audit examined the document authentication processes; financial processes; service to the public; information systems and information security; the digital apostille; and the National Digital Agency's self-service kiosks for government services.

---

## Key Findings



### Deficiencies in the Authentication Processes for Public Documents



**Work Procedures for the Document Authentication Process** – The Ministry of Foreign Affairs conducts an official authentication process for hundreds of thousands of documents each year and issues apostille certificates for them (323,000 in 2024), in accordance with its obligations under the regulations and the Convention. It was found that the Ministry operates without having formalized the process for handling requests for apostille certificates in written procedures, contrary to the provisions of the handbook on the implementation of the Convention and contrary to its administrative obligations. Establishing written procedures for the document authentication process and ensuring their strict implementation could have prevented significant deficiencies identified in this audit. Among other things, such procedures could address the mode of operation, methods of implementation, and oversight measures for document authentication, payment of the fee, issuance and registration of the apostille, assurance of service quality, staff training, and fraud detection. The purpose of regulating these activities is to ensure uniform, authorized, controlled, and efficient performance in accordance with the Apostille Convention, and to reduce the possibility of undesirable actions such as discrimination and embezzlement. In the absence of detailed work procedures, the oversight processes required for this sensitive process are also impaired.

 **Verification of the Signatures of Authorized Signatories** – The information system used by the Ministry of Foreign Affairs to issue apostille certificates lacks specimen signature images for 45% of the authorized government signatories recorded in the authentication system (2,259 out of 4,979). As a result, the Ministry issued apostille certificates even though it was unable to carry out, as required, the authentication process for documents signed by authorized signatories and to perform the required visual comparison of signatures. Nor did it carry out any alternative checks to confirm the authenticity of the signature as part of the apostille issuance process. From January 2022 to June 2024 (the audited period), the Ministry of Foreign Affairs issued 160,294 apostille certificates for public documents signed by authorized signatories without being able to perform the required comparison of signatures, since their specimen signatures were not present in the system. This represents approximately half (50%) of all certificates (318,604) issued for documents bearing the signature of an authorized signatory during the period examined. It was also found that even when a specimen signature was present in the authentication system, it was not checked, and no comparison between the signatures was actually performed. The Ministry of Foreign Affairs' failure to ensure a visual comparison of signatures as part of the document authentication process – intended to verify the authenticity of the document, in accordance with the practice described in the handbook on the implementation of the Convention – and its failure to carry out any alternative verification process constitute a failure by the Ministry to fulfill its responsibilities in the field of apostille issuance.

 **Authentication of Population Authority Documents** – Since 2019, most documents issued by the Population Authority have been stamped with the Authority's seal (rather than signed by an authorized official). Regarding Population Authority documents, the following was found:

- The Ministry of Foreign Affairs approves Population Authority documents without performing the checks required to verify the document against a specimen seal, identifying markers, or security features, and without conducting a visual comparison of the document and the seal in accordance with the practice described in the handbook on the implementation of the Convention. It should be noted that observations conducted by the State Comptroller's Office also found that apostille certificates were issued for such documents without comparison, verification, or examination of these characteristics.
- In the information system used to issue apostille certificates, the Ministry of Foreign Affairs does not maintain specimen seals, identifying markers, or security features of Population Authority documents. As a result, from January 2022 to June 2024 the Ministry issued 367,859 apostille certificates for such documents – approximately 53% of all apostille certificates issued (687,848) – without performing the authentication process as required.
- The Ministry of Foreign Affairs issued apostille certificates for Population Authority documents even for photocopies of Population Authority documents, which were not original documents and were printed on ordinary paper. Issuing apostille certificates for non-original Population Authority documents without proper verification of the seal and other identifying features creates a serious risk that the Ministry of Foreign Affairs may fail to detect a forged document before issuing the apostille certificate.

- The Population Authority's use of special paper containing security features intended to prevent forgery and to enable the detection of photocopies is implemented only partially and only at self-service stations. By contrast, documents issued in person by a Population Authority clerk or sent by mail at the request of a citizen are printed on paper that does not contain security features; therefore, there is no way to determine whether the document has been photocopied or forged. The Population Authority's conduct in this regard undermines the reliability of these documents and their protection against forgery, as well as the ability of the Ministry of Foreign Affairs to authenticate documents in accordance with the Apostille Convention and the regulations.

 **Authentication of Printouts of Digital Documents** – Apostille certificates for digitally signed documents that require authentication through a digital process cannot be issued on the basis of a printed copy, but only on the basis of the electronic file. It was found that the Ministry of Foreign Affairs also issued apostille certificates for digital public documents that were printed and presented only as hard copies, without requiring the submission and examination of the electronically signed digital file for the purpose of verification or comparison as part of the authentication process. In addition, in a random customer test conducted as part of the audit, the Ministry issued an apostille for such a document that had even been photocopied prior to submission for authentication, without the applicant being required to present the electronically signed digital file. It follows that the Ministry of Foreign Affairs authenticates and issues apostille certificates for printed copies of public documents originally signed digitally, even though such signatures are relevant only to the digital original. Since no examination or comparison of the printout or its source is carried out, these printouts cannot be authenticated as required under the Apostille Convention, and apostille certificates should not be issued for them under the handbook on the implementation of the Convention and the guidelines of the Population Authority.

 **Authentication of Public Documents without Visual Comparison** – The share of apostille certificates issued for documents for which the signatures of authorized signatories or the seals of the public body do not appear at all in the system is 77% (529,538) of all certificates issued (687,848). This is in addition to certificates issued without performing a visual comparison even where the signature does appear in the system, as observed in the audit. The Ministry of Foreign Affairs' practice of issuing hundreds of thousands of apostille certificates without carrying out the authentication process as prescribed in the handbook on the implementation of the Convention – and without any alternative procedure to ensure the authenticity of the document – constitutes a serious deficiency that may undermine other countries' ability to rely on apostille certificates as assurance that the documents are not forged. The implications of requesting an apostille on the basis of a forged document are broad and significant, affecting both domestic administrative integrity and international obligations under the Apostille Convention, which is intended to enable the 127 Contracting Parties to rely on certification by a competent authority of another signatory state that the public document presented has been duly authenticated.

 **Completeness and Currency of Authorized Signatory Data** – The audit found that signatures of authorized signatories submitted by public bodies to the Ministry of Foreign Affairs for comparison in the authentication process were not scanned into the authentication system for many months, and in some cases were not scanned at all. For example, approximately 400 specimen signatures of authorized signatories submitted by the Ministry

of Religious Services at the beginning of 2023 had still not been scanned into the system due to "staff shortages." An analysis of system data showed that 47,452 apostille certificates were issued for documents of the Ministry of Religious Services bearing the signatures of these authorized signatories, even though their signatures were not in the system and no comparison of signatures was performed. It was further found that for 51% of all authorized signatories in the system (2,554 out of 4,979), essential information is missing and the data is incomplete. For example, some records lack the affiliation to the public body or the first name, without which proper verification of the document signatory cannot be carried out.

### **Practice of Issuing Certificates that Undermines the Integrity and Reliability of the Apostille Register**

– The audit found that, in order to save time in providing service, the Apostille Department issued dozens of apostille certificates daily in advance and in batches, with all apostille details pre-filled except for the manual signature of the Ministry of Foreign Affairs representative, for use in future requests from occasional applicants. This practice prevented proper recording or association of a specific apostille with a specific applicant or public document for which it was actually issued. An analysis of the register database showed that most apostille certificates (87% – 599,875 out of 687,849) were issued within no more than one second of the issuance time of other apostille certificates in the register. Since the issuance process takes several minutes, this finding indicates an improper process, resulting at least in part from the batch issuance of certificates. This practice of issuing apostille certificates in advance had negative consequences, as the register entries for those certificates do not accurately reflect the issuance process. The conduct of the Ministry of Foreign Affairs undermines the integrity and reliability of the register and impairs the ability of countries party to the Convention to exercise their right to compare the issued apostille with the register details, contrary to the purpose of the register as a tool for preventing fraud. In addition, the inaccurate records prevent the Ministry's management from deriving relevant information from the register for management, data analysis, service improvement, and informed decision-making based on the register data.

 **Apostille Certificates Issued for Criminal Record Certificates** – The Police send criminal record certificates to foreign embassies in Israel, which return them to the applicant with a request to obtain an apostille. During the audited period, the Ministry of Foreign Affairs issued tens of thousands of apostille certificates for such documents (at least 20,248 from January 2022 to June 2024) and delivered them directly to the applicants or their representatives. As a result, the conduct of the Police and the Ministry of Foreign Affairs is inconsistent with the provisions of the Criminal Information Law, in a manner that may allow the leakage of information and its misuse, risks that the law was intended to prevent. The Ministry of Foreign Affairs explained to the audit team that it is aware that its actions are inconsistent with the purpose of the law, but that it has no alternative, as embassies return the certificates directly to citizens so that they can independently obtain apostille certificates.

 **Self-Service Kiosks for Government Services** – The operation of 28 out of 284 kiosks operated by the National Digital Agency was examined. It was found that 36% (10 out of 28) of the kiosks examined were malfunctioning, and it was not possible to obtain services for printing various government certificates. From 2023 to the end of April 2025, 29,952 population registry extracts were issued through self-service kiosks.

- It was found that in one-third (33%) of the operational kiosks (6 out of 18), official government certificates (such as population registry extracts and vehicle information) were printed on plain paper, without the State emblem and without any security features intended to prevent the use of forged documents and to ensure reliance on original official documents. It was also found that the Ministry of Foreign Affairs issued apostille certificates for population registry extracts even when they were printed on plain paper, despite the fact that their authenticity could not be verified and without performing any other action to verify their authenticity. It was further found that the use of plain paper is not known to the relevant government bodies responsible for ensuring that services are provided without vulnerabilities that expose them to forgery.
- It was found that only 5 of the 18 kiosks (28%) issued Population Authority certificates on paper with security features designated for Population Authority documents. In the remaining operational kiosks, certificates were printed on plain paper, as noted, or on paper with other security features.
- It was found that in the pharmacy chain where approximately 120 self-service kiosks are located, branch staff hold keys to the kiosks and use them to release print jobs in cases of minor malfunctions and to replenish paper in the printers inside the kiosks. This situation – allowing numerous, varying, and unidentified employees practical access to kiosks containing a sensitive government computer and blank official paper with built-in security features, on which a range of official certificates can be printed and which constitute *prima facie* evidence of their authenticity – poses a significant risk of misuse, embezzlement, and fraud.
- Moreover, one kiosk examined was found unlocked, and in another the key was left in the lock. In these kiosks, audit staff were able to open the units and access their sensitive contents without restriction. In addition, during inspections of kiosks at various branches, pharmacy staff opened the kiosks for the State Comptroller's Office staff and showed them their contents and the sensitive paper inside, without requiring them to identify themselves or state their role. In some branches, pharmacy staff stated that they opened the kiosks to load plain paper when the printer ran out of paper, even when the trays designated for official government paper were empty.
- It was found that there is a significant information security vulnerability that allows actors with malicious intent to take control of the kiosks and carry out actions to issue certificates, posing a real risk of misuse and fraud.
- It was found that the National Digital Agency, which operates these kiosks, does not monitor the use of official paper with security features and does not conduct periodic reconciliation or any other control comparing the quantity of such paper with the number of certificates actually issued, in order to prevent misuse. The audit findings indicate that in many cases printing was carried out on plain paper without the knowledge of the National Digital Agency, further exacerbating the control deficiency and the lack of information regarding the use of surplus official paper. In addition, a significant deficiency was found in the National Digital Agency's physical security measures for the kiosks and access to their contents, which enabled misuse and additional information security risks.

The findings described above reflect deficiencies in the management, oversight, and control exercised by the National Digital Agency over the self-service kiosks. This conduct, beyond impairing service to the public, creates

a real risk of misuse and could facilitate the trade and production of forged official government paper, with all its implications.

## Financial Aspects of Apostille Issuance

 **Lack of Reconciliation between Payment Systems and Ministry of Foreign Affairs Systems** – The audit found that, contrary to the provisions of the Government Financial Regulations (TAKAM), there are in practice no interfaces between the Ministry of Foreign Affairs' operational system and the actual payment data. In the authentication system, in which fee payment details for apostille issuance are entered, there is no link or interface to the payment systems through which the fees are actually paid, neither the Government Payment Service nor the Postal Bank. It was also found that the Apostille Department has no access to payment system data, either in real time or retrospectively. It was further found that although barcode scanners were installed at the Ministry of Foreign Affairs to read receipt numbers and amounts from receipts issued by the Government Payment Service (intended to prevent manual data entry errors) they were not used, and the data was entered manually. A discrepancy was found in 9.2% of the receipts recorded in the authentication system (6,542 out of 71,173) compared with the receipts actually issued by the Government Payment Service. The recording practices in the authentication system, together with the absence of input and processing controls in the receipt intake process, allow for data entry errors and create an opening for fraud and embezzlement, without preventive or compensating control mechanisms in place. Moreover, it was found that 76% of the receipts for which no match was found do not exist at all in the Government Payment Service (5,005 receipts), with a cumulative amount of approximately NIS 970,000 recorded in the authentication system. The remaining unmatched receipts include amounts higher than those recorded in the Government Payment Service, totaling approximately NIS 130,000. The total discrepancy for the period examined is therefore approximately NIS 1.1 million. This finding reflects a significant deficiency in the Ministry of Foreign Affairs' management of public funds, error control, and measures to prevent fraud and embezzlement.

 **Accounting Irregularities in Apostille Fee Revenues** – In the years 2022–2024, 836,626 apostille certificates subject to payment were issued in the authentication system, for which the total fees payable under the regulations amount to approximately NIS 31.4 million. The audit found that the Finance Division of the Ministry of Foreign Affairs does not receive or review the financial data managed in the authentication system; does not request or obtain data on the actual volume of apostille certificates issued; does not reconcile apostille fee revenues with the volume of services provided by the Apostille Department; does not assess the reliability of the system data or its recording; and does not examine the propriety of the financial processes or their implications. All of this is contrary to the Government Financial Regulations (TAKAM), government accounting standards, principles of proper administration, and the measures required for the prevention of fraud and embezzlement.

 **Collection of Apostille Fees at Lower-than-Prescribed Rates** – The audit found that, contrary to the regulations, the fee rate for apostille certificates issued by the Ministry of Foreign Affairs during the audited period (January 2022 to June 2024) was set at NIS 38 instead of NIS 39, as published on the Ministry's website, published and collected by the Government Payment Service, and calculated in the authentication system. The rate was updated to NIS 39 only in December 2024, during the audit period, with a delay of nearly one year. An analysis of

authentication system data further showed that in previous years as well, when the fee rate was updated in the regulations, the updated rates were not implemented by the Ministry of Foreign Affairs in a timely manner. It was found that approximately 65% of the receipts (47,471 out of 73,209 for the audited period – January 2022 to June 2024) were recorded in the system at fee rates lower than those prescribed in the regulations. The cumulative financial gap resulting from the failure to update the fee rate in a timely manner during the audited period amounts to approximately NIS 1 million in lost revenue to the State Treasury.

## Service to the Public in the Authentication of Public Documents



**Limited Availability of Apostille Services** – As of May 2025, document authentication services are provided only at the Ministry of Foreign Affairs office in Jerusalem, for just three and a half hours in the morning. The Ministry no longer allows documents to be deposited in designated drop boxes in Tel Aviv, Haifa, and Be'er Sheva as in the past, despite growing demand over the years, which reached more than 300,000 certificates in 2024. This situation requires thousands of citizens from across the country to travel to Jerusalem in the morning, wait for service without the possibility of booking an appointment in advance, and in many cases wait for several hours standing outside the Ministry's gates – without shade, without adequate seating, and without access to water or restrooms – or alternatively to rely on courier services whose cost is hundreds of percent higher than the statutory fee. The limited service provided by the Ministry of Foreign Affairs, restricted in hours and days and available at only one location nationwide, has impaired the quality and accessibility of the service for those who require it.



**Appointment Scheduling for Services at the Ministry of Foreign Affairs Office in Jerusalem** – The option to schedule appointments at the Ministry of Foreign Affairs office in Jerusalem was opened once a month, on the first working day of each month, for appointments in the following month. The audit found the following:

- The number of appointments allocated to the general public declined by approximately 80% in the years 2023–2024. While an average of approximately 30,000 certificates were issued per month, the Ministry allocated only approximately 550 appointments, forcing applicants to seek alternative channels, including paid courier services.
- In 2024, the average time between the opening of appointment slots each month and the booking of all available appointments was less than two minutes. As a result, applicants who were not aware of the appointment release mechanism had virtually no chance of securing an appointment for apostille services.
- It was found that 72% of appointments in 2024 were booked by individuals who reserved at least 10 and up to more than 100 appointments each during that year, reflecting large-scale booking of appointments, typically by couriers. It was also found that the primary recipients of services at the public reception desk were couriers who were granted access without appointments. The absence of an effective control mechanism allowed couriers and other actors to continue accumulating appointments without limitation, thereby restricting private citizens' access to the service.
- In August 2024, the Ministry of Foreign Affairs canceled the option to schedule appointments. As a result, for nearly ten months it has not been possible to book an appointment in advance for document authentication services.

 **Queue Management Kiosk** – It was found that the local queue management kiosk has not been operated on a regular basis since 2020 to manage the flow of service recipients. As a result, applicants are required to wait for hours to receive service, often holding two queue numbers. The absence of a local queue management system covering all stages of the waiting process has led to disorder in the reception of the public and prolonged waiting times, with applicants standing outdoors in the open air.

 **Receipt of Apostille Services through Private Service Providers (Couriers)** – The Ministry of Foreign Affairs has not made appropriate preparations for providing document authentication services and has not managed public access to this service in an equitable manner. Its conduct has enabled couriers to take over reception hours within this public service, to the detriment of citizens waiting their turn and in violation of their right to receive fair and equal service from a government ministry, as well as the principle of equal access to public services. The widespread reliance of service recipients on courier services significantly increases the cost borne by applicants, since the cost of authenticating a single document through a courier ranges from NIS 300 to NIS 1,000 – hundreds of percent above the statutory government fee of NIS 40 that applicants would have paid had accessible and available government services been provided. This situation is necessarily the result of the deficient service provided by the Ministry of Foreign Affairs. The audit further found:

- Couriers received service even without an appointment. Moreover, on-site security staff were unable to prevent their entry into the reception hall despite their lack of appointments, and when attempts were made to block their entry, service providers in the division contacted security staff by phone to request that they be admitted.
- The limit set by the Ministry of Foreign Affairs of up to ten documents per applicant was not enforced with respect to couriers. Processing their requests took a considerable amount of time, while the few citizens who managed to secure appointments in advance were required to wait for extended periods at the entrance to the Ministry.
- Couriers were observed openly offering citizens waiting outside the reception hall to authenticate documents on their behalf for a fee of hundreds of shekels, taking advantage of their unrestricted access to service counters.

It follows that the amount paid by citizens for courier services was at least NIS 50 million<sup>9</sup> in 2023 alone, representing excess payments of approximately NIS 45 million.

 **Availability of the Telephone Service Center** – In March 2025, the number of days on which telephone service was available was reduced from three days to only two days per week, during afternoon hours. It was found that, on average, about 70% of incoming calls on service days went unanswered, and in March 2025 only 6% of calls were answered. It was further found that on 38 days during this period when telephone service was available, none of the incoming calls were answered, and a total of 4,499 callers waited in vain for a response. The lack of an effective and structured telephone service for document authentication – and, more seriously, the complete absence of any response over entire

---

<sup>9</sup>

Based on an average price of approximately NIS 400 per document.

days – impairs the availability of services to the public, deepens feelings of frustration and distrust in state institutions, and may even be perceived as disregard for the government's obligations toward the public.

 **Accessibility of Information for Apostille Service Applicants** – The audit found that the information available to the public online regarding apostille services is not presented in an adequate or user-friendly manner: it is spread across multiple pages; there is no consistency between the different pages; and the information is partial, incomplete, and incorrect. For example, on the Israel Police website, the fee is still listed as NIS 38, and there is no distinction between criminal record certificates intended for countries that are parties to the Apostille Convention and those intended for countries that are not. On the Ministry of Justice website, in the section on digital apostilles, there is no transparency regarding the fact that some countries that are parties to the Apostille Convention do not accept apostilles in this format. On a page on the Ministry of Foreign Affairs website, it is stated that "the fee for authentication of each document is NIS 40," despite the fact that no fee should be charged for documents not intended for countries that are parties to the Apostille Convention. The absence of a clear distinction between document authentication for countries that are parties to the Convention and those that are not, where no fee should be charged, leads applicants to pay fees unnecessarily. These deficiencies in the presentation of information constitute a tangible impairment in the quality and accessibility of apostille services provided to the public.

## The Digital Apostille

 **The Digital Apostille** – Despite a 2020 government decision to establish, within four months, an infrastructure enabling all relevant government ministries and public authorities to issue digital authentication for public documents provided electronically, implementation has been highly partial. Actions taken to date have resulted in only minimal use of the digital apostille: (a) the Ministry of Justice launched the service only after approximately two years; (b) as of the time of the audit – approximately five years after the government decision – only 5 out of approximately 60 bodies had joined the digital apostille service; (c) the number of public documents made available for digital apostille stands at only 11, out of dozens of potential documents; (d) five years after the government decision, the use of digital apostilles accounted for less than 1% (0.8%) of all apostilles issued in Israel – only 7,100 digital apostille certificates out of 854,000 total certificates issued in 2022–2024. This is despite the Ministry of Justice's target that by the end of 2024, 70% of commonly issued public documents in Israel would be eligible for digital apostilles; (e) the Ministry of Justice applied the service only to the issuance of digital apostilles and not to the certification of public documents for countries that are not parties to the Apostille Convention, as required by the government decision.

The audit further found that citizens who obtained digital apostilles encountered refusals by various countries that are parties to the Apostille Convention, or by entities within such countries, to accept the digital apostille. These citizens were required to order the original (non-digital) document by post or go in person to the relevant government office, and then undergo the process of obtaining a physical apostille at the Ministry of Foreign Affairs in Jerusalem, including making an additional payment for a service they had already paid for. It was also found that the Ministry of Justice's information page for this service provides no transparency regarding countries or entities that do not accept digital apostilles. In addition, the Ministry of Justice does not operate a customer service center responsible, *inter alia*, for assisting citizens encountering difficulties in using digital apostilles in destination countries.

 **Adjustment of the Digital Apostille Fee** – A transaction carried out in person at a service desk costs up to 50 times more than a digital transaction, thus rendering, the cost of issuing a digital apostille significantly lower than the cost of operating the manual apostille service. Despite this and the clear interest in encouraging and expanding the use of digital apostilles – *inter alia*, to reduce costs for both the government and the public – the fee for a digital apostille is identical to that for a manual apostille (NIS 40). As a result, the current fee structure does not fulfill the purpose of the government decision to set differentiated fees based on the considerations set out therein.

## Information Security and the "Imutim" Information System

 **Sharing of Passwords and User Accounts** – The audit found that usernames and passwords for user accounts in various information systems of the Ministry of Foreign Affairs and other public bodies were visible to all, written on notes affixed adjacent to service workstations in the Apostille Department; some were even visible to the service recipient. Moreover, several staff members in the Apostille Department were found to have acted in clear violation of information security rules and of the principles of confidentiality and protection of government information, in a manner that did not allow any oversight of their activities. The exposure of usernames and passwords, and the failure to uphold confidentiality and personal accountability, may lead to the exposure, theft, alteration, or destruction of information, without the Ministry of Foreign Affairs being able to identify the individual responsible.

 **Deficiencies in the Operation of the "Imutim" System and the Need for Control Processes** – The audit identified fundamental gaps across a range of areas: from partial and inadequate system design and input processes, through deficient use and entry of required and desired data fields, to flawed processing procedures and inadequate management of the sensitive database maintained in the system, which contains incomplete, incorrect, and missing data. The accumulation of these deficiencies, and the risks they create in handling a sensitive domain with international implications, could amount to professional negligence in the functioning of the department.

---

## Key Recommendations

### Gaps in the Authentication Processes of Public Documents



The Ministry of Foreign Affairs should formalize the entire public document authentication process in a detailed procedure that sets out instructions for all stages of the process, in accordance with the Apostille Convention and the regulations, including the issuance of apostille certificates and the use of the information system. The Ministry should also implement consistent control processes to ensure that the Apostille Department operates in practice in accordance with the procedures to be established.



The Ministry of Foreign Affairs should immediately update the database of the Imutim System and ensure that it includes all authorized signatories and their specimen signatures for those authorized to sign public documents in the executive branch. This is in addition to its obligation to maintain an orderly mechanism for periodic and ongoing updates of authorized signatories. The Ministry should also ensure that, in the approval of public documents signed by authorized signatories, authentication staff perform signature comparisons between the signature appearing on the public document and the specimen signature in the Imutim System. It is further recommended that the Ministry consider incorporating automated technologies for signature identification and comparison, such as artificial intelligence tools.



The Ministry of Foreign Affairs should ensure that the required authentication process is carried out when approving documents issued by the Population Authority. In this context, it is recommended that the Ministry consider using the Population Authority's information system ("Aviv") to verify the source of the public document submitted for authentication, as part of the authentication process, in addition to the measures described above. The Ministry should also prepare a professional guide containing instructions for all types of documents issued by various bodies, based on their guidelines and those of the Population Authority, including paper specifications, types of stamps, and other identifying features, including security features used to ensure the reliability and authenticity of Population Authority documents. In addition, the Ministry should include in the Imutim System the specimen stamps used by the Population Authority in issuing certificates to the public.



In an era in which imaging and editing technologies are widely accessible, including through the use of artificial intelligence tools, the ability to forge documents has become easy and readily available. The Population Authority, in cooperation with the Ministry of Foreign Affairs, should upgrade the existing protections in the paper currently used by clerks in offices and for documents sent by post. In this context, it should take into account that under the current conditions, due to the absence of protections and watermarks, documents issued on this paper can be copied or forged without Ministry of Foreign Affairs officials being able to detect this.



The Ministry of Foreign Affairs should refrain from issuing apostille certificates for printed copies of digitally signed documents unless they have undergone a proper authentication process as set out in the aforementioned procedure, such as examining the original electronically signed file with a legally recognized signature and comparing the printout with its content, or using the "Aviv" information system as noted above. In addition, the Ministry of Foreign Affairs, *inter alia*, through the Consular Division, should conduct a thorough review of its practices regarding the issuance of apostille certificates, while establishing rigorous control mechanisms, in addition to structuring periodic training processes on the Convention, its implications, requirements, and implementation, and streamlining procedures, including through digitization, all in order to ensure that the Ministry fulfills its obligations under the Convention.



To enable accurate authentication through the authorized signatories database, the Ministry of Foreign Affairs should conduct a regular periodic process with public bodies to verify the accuracy, completeness, and currency of all relevant information regarding authorized signatories in the Imutim System. This should also ensure the ongoing receipt of up-to-date information on the terms of office of authorized signatories from each public body, both upon their appointment and upon the conclusion of their role, or in advance of its expected completion date, as required under the Convention implementation handbook and principles of proper administrative practice. Public bodies should update the Ministry of Foreign Affairs upon the appointment and termination of each authorized signatory.



The Ministry of Foreign Affairs should ensure the maintenance of a complete and reliable register and verify that each apostille certificate is issued specifically and individually for a particular public document submitted for authentication, and only after the authentication process has been properly completed in accordance with an orderly procedure. The Ministry should also ensure that the data relating to issued apostille certificates, both in the register and in the Imutim System, are complete, accurate, and reliable.



It is recommended that the Ministry of Foreign Affairs and the Israel Police clearly present to the public the legal provisions and required procedures in cases where an apostille is needed for a criminal record certificate. It is proposed that the relevant bodies consult with the Ministry of Justice in order to design an optimal process that complies with both the provisions and the purpose of the law. For example, in cases where issuance of a physical certificate is required, the Israel Police could send all criminal record certificates requested for submission to a foreign country directly to the Ministry of Foreign Affairs, rather than to the foreign embassy. Following authentication and issuance of the apostille, the Ministry of Foreign Affairs would send the certificates to the Israeli embassy in the destination country or to the competent authority in that country, thereby ensuring compliance with the law and preventing the applicant from obtaining the certificate.

## Self-Service Stations for Government Services



The National Digital Agency should re-examine the operating model of the self-service stations for government information. It should establish clear procedures for their operation and for their physical and logical protection, including the development of digital control mechanisms to monitor the use of official paper and the periodic flagging of irregularities in such use. The Agency should ensure that only the appropriate paper is loaded for each type of certificate or document, so that each output is produced exclusively on its designated paper, including the specific security features of each issuing body, and that plain paper is not used for printing official documents. In addition, the National Digital Agency should ensure that access to the self-service stations and their software components is hardened, and that the necessary measures are taken to prevent unauthorized actors from producing official documents, thereby reducing information security risks, unauthorized access to official paper bearing security features, and opportunities for fraud and misuse.



In view of the high number of cases in which self-service stations for government services were found to be malfunctioning, the National Digital Agency should improve its handling of all types of faults in the stations and ensure their proper and continuous operation, including adherence to appropriate response times that would enable uninterrupted service to the public and improve overall service quality.



The Population Authority should provide the Ministry of Foreign Affairs with clear guidance regarding the security features of the population registry extract. Accordingly, the Ministry of Foreign Affairs should verify these features as part of the authentication process for such documents and ensure that apostille certificates are issued only for Population Authority documents that comply with the Authority's guidelines and specifications.

## Financial Aspects of Apostille Issuance



The Ministry of Foreign Affairs, in cooperation with the National Digital Agency, should implement the provisions of the Government Financial Regulations (TAKAM) by establishing real-time computerized interfaces between the Imutim System and all other relevant operational systems and the payment systems. Implementing such integration would ensure the accuracy of payment data, reduce the potential for manual errors in service delivery, fraud, embezzlement, and receipt forgery, and shorten processing times for each request, thereby improving the efficiency and reliability of service and financial processes in the Apostille Department and the Ministry of Foreign Affairs.



The Ministry of Foreign Affairs should incorporate the financial aspects of apostille issuance and the use of barcode scanners into a formal procedure governing service delivery in the Apostille Department. In addition, the Ministry should implement automated controls to validate input data during receipt entry and conduct periodic processing controls, both automated and manual, over financial processes to ensure their

reliability, the proper recording of data, and its accuracy, including through automated reconciliation with the Government Payment Service and the Postal Bank. The Ministry should also establish structured reports to flag irregular activities for use in the oversight processes of the Finance Division and the Ministry's management.



The Ministry of Foreign Affairs should carry out ongoing controls and monitoring to ensure financial reconciliation between the data on apostille issuance outputs and the payment data received through the various payment channels and transferred to the Ministry of Finance. It should also conduct periodic reviews to identify potential irregularities and ensure that data are accurately and reliably reflected in the systems, and that the Finance Division complies with the provisions of the Government Financial Regulations (TAKAM) and the government accounting standard regarding the recognition, measurement, and recording of assets and liabilities arising from apostille fees, as well as oversight and control of information systems containing financial data.



The Ministry of Foreign Affairs, through its Finance Division, should implement the provisions of the Government Financial Regulations (TAKAM) for mapping all charges under the Ministry's responsibility, in cooperation with the Legal Department and the relevant professional units, and ensure that fee rates are updated in accordance with the legal basis for each charge at the beginning of each year. It is recommended that the Ministry establish and implement a procedure for updating the apostille fee in all relevant channels, including publication on the Ministry's website and various information sites, in the Imutim System, in the Government Payment Service system, in the procedures of the Apostille Department, and in staff training. This is to ensure that the fee is updated at the start of each year in proximity to the publication of the regulations, in accordance with their provisions, and that implementation of the procedure is monitored. In addition, the Israel Police should update the current apostille fee in its online information pages and ensure that it is revised promptly following any change to the fee set out in the regulations.

## Service to the Public in the Authentication of Public Documents



The Ministry of Foreign Affairs should adapt its services to the growing demand in order to enable applicants to receive accessible and available document authentication services in accordance with the government service framework, without requiring them to send original documents by post or rely on courier services. To this end, it is recommended that the Ministry consider extending operating hours to include afternoon hours, reinstating (in cooperation with the Population Authority) the option of depositing original documents in designated drop boxes at government offices across Israel, and alternatively providing in-person services at additional locations across the country. It is also proposed that the Ministry consider employing courier and postal services for the delivery of original documents and their return with an apostille, in order to provide applicants with a secure and efficient service.



The Ministry of Foreign Affairs should ensure that document authentication services are provided in an equitable and accessible manner and prevent companies and private individuals from commercializing this service at the expense of citizens. In this context, it should ensure that: (a) couriers are subject to limits on the number of documents they may submit, similarly to other applicants; (b) payment of fees in the public services area is enabled via a kiosk operated by the National Digital Agency, which is continuously available and provides verified information; (c) clear signage is displayed in the reception hall encouraging citizens to use the kiosk; (d) no preference is given to couriers over individual applicants, including in the allocation of service counters; and (e) no parallel commercial activity takes place at the Ministry's premises. The Ministry should conduct periodic and digital controls in the queue management system to ensure that these practices are eliminated.



The Ministry of Foreign Affairs should provide an adequate telephone service during the hours set out in the government service framework, ensure that all callers receive a response, and verify that the telephone service position is staffed on all days for which telephone service has been advertised.



It is proposed that the Ministry of Foreign Affairs and the Ministry of Justice, as the competent authorities for issuing apostille certificates, in cooperation with the National Digital Agency – the body responsible for improving digital interfaces and government services – establish a unified information page consolidating all information relating to government activity in the field of document authentication. This would make all relevant information, as well as both digital and in-person service options for the authentication of public documents and the issuance of apostilles, accessible to applicants. The competent authorities should update this information on an ongoing basis in line with developments in the field and changes in legislation, including with respect to fee rates.

## The Digital Apostille



The Ministry of Justice, in cooperation with the National Digital Agency, should work with the relevant government ministries to complete the development process and connect all relevant government bodies and documents to this digital service. It should also promote public awareness of the service and its benefits, including by improving the accessibility of information on the government services website. In addition, the Ministry of Justice, in cooperation with the Ministry of Foreign Affairs, should continue working with countries that are parties to the Apostille Convention to remove barriers and enable the use of digital apostilles issued in Israel. So long as some countries do not accept digital apostilles, the Ministry should update its website to indicate which countries accept them and which do not.



It is recommended that the Ministry of Justice, in cooperation with the Interministerial Fees Committee and the Ministry of Finance, adjust the fee for issuing a digital apostille, in light of the reduced government resources required for its issuance and in order to encourage public use of the service. This would improve service delivery and significantly reduce government expenditure on manual apostille issuance, as reflected in relevant government decisions.



If, at present, it is not possible to provide an adequate solution to the public through the digital apostille, it is proposed that the Ministry of Foreign Affairs, in cooperation with the National Digital Agency and the Ministry of Justice, consider a technological project based on the Government Data Exchange Infrastructure and the "once-only" principle. Such a project would enable citizens to request apostilles digitally for the required documents, pay for them online, and have service providers in government ministries or the Ministry of Foreign Affairs procure the original document directly from the relevant government system, issue the apostille, and send the document together with the apostille to the citizen by post. Such a system could improve document authentication, prevent forgery, and provide efficient, high-quality service to the public. To this end, it is proposed that the Minister of Justice consider authorizing civil servants in bodies with high demand for document authentication, such as the Population and Immigration Authority and the Israel Police, and designating those bodies as competent authorities for issuing apostille certificates.

### **Information Security and the "Imutim" Information System**

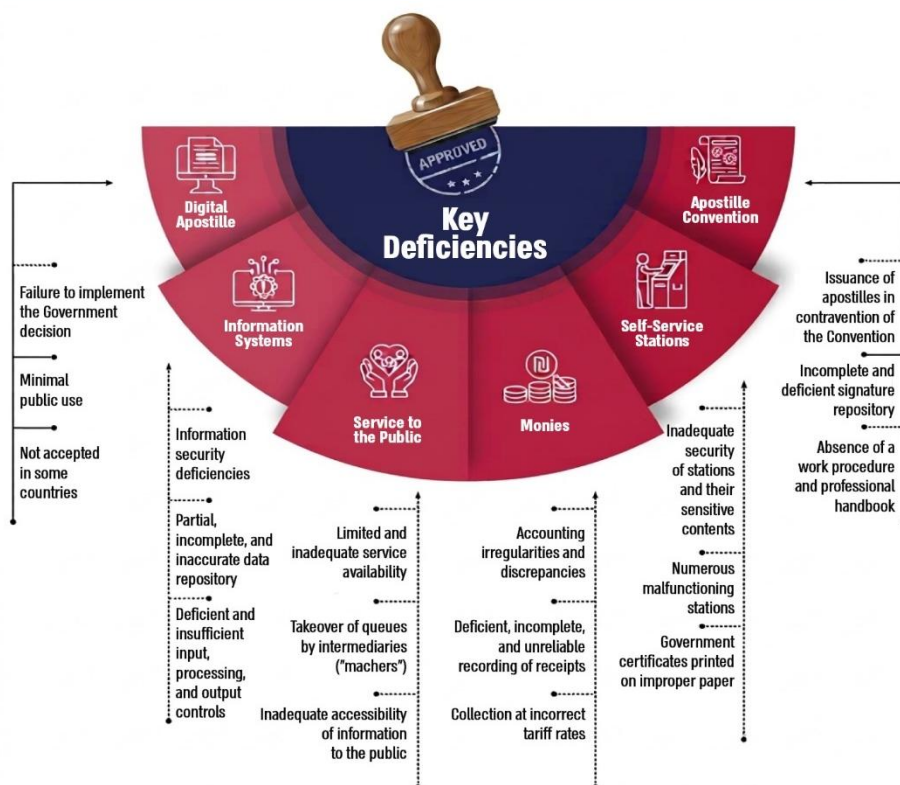


The Ministry of Foreign Affairs should promptly address the information security gaps identified and reinforce the binding information security procedures in the Apostille Department, as well as conduct periodic controls to ensure their implementation.



The Ministry of Foreign Affairs should address the management of the document authentication process within the Imutim System. This includes re-specifying the system, updating it, incorporating mandatory fields and input, output, and processing controls, and improving the quality of the existing database. The Ministry should also develop a practical user guide for system users, setting out the required processes, methods of operation, and necessary information, and reflect all of these in comprehensive and detailed work procedures for the Apostille Department.

## Key Deficiencies in Document Authentication Services



---

---

## Summary

In today's globalized world, where people, information, and documents frequently cross borders, the need for international cooperation in regulating bureaucratic processes is increasing. The Apostille Convention, drafted by the Hague Conference on Private International Law (HCCH) – an intergovernmental organization whose purpose is the progressive unification of the rules of private international law – was signed in 1961 and is intended to simplify the process of authenticating public documents between countries. The Convention established a uniform mechanism for the authentication of public documents, under which an apostille is issued by a competent authority in the country where the original document was issued, certifying the authenticity of the signature, seal, or stamp, and is recognized in all countries that are parties to the Convention. As of March 2025, 127 countries, including Israel, are parties to the Convention. An apostille is required when public documents are needed in foreign countries, for example for obtaining foreign citizenship, professional licensing, employment, and matters relating to personal status. This process ensures uniformity, reliability, and efficiency in international document authentication, and enables countries to rely on apostilles for the recognition of public documents issued abroad.

This report examines the conduct of the Ministry of Foreign Affairs with respect to the authentication of public documents and the issuance of apostille certificates, which amounted to approximately 323,000 certificates in 2024. It was found that the Ministry operates in this area of international law without a formal procedure or operational guide. At the core of its activities in this field – the authentication process – the Ministry does not fulfill its obligations under the Convention, and significant deficiencies were identified. In the financial domain of fee collection and management, accounting irregularities and discrepancies were found, as well as deficient, incomplete, and unreliable recording of revenues amounting to millions of shekels, a lack of reconciliation between revenue systems and Ministry systems, and under-collection of fees. In the area of public service, significant deficiencies were found, including the provision of limited services that fail to comply with the government service framework. As a result, many applicants rely on courier services and pay tens of millions of shekels annually. In the area of information security and information systems, substantial deficiencies were identified, indicating negligence in the work of service providers within the Ministry of Foreign Affairs, resulting in an information system containing incomplete, missing, and even incorrect data.

The Ministry of Foreign Affairs should comprehensively review all aspects of the process for authenticating public documents and issuing apostille certificates, and should establish a formal procedure and a guide for service providers covering the entire service process and the use of the information system. The Ministry should also establish a professional system of controls – operational, financial, and accounting – to ensure that the significant deficiencies identified in this report are rectified promptly and do not recur, and to maintain the confidence of countries that are parties to the Apostille Convention in the quality and professionalism of the certificates issued by the Ministry.

The digital apostille project, managed by the Ministry of Justice in accordance with the Government decision, has the potential to simplify the process of document authentication and apostille issuance, significantly reduce the Ministry of Foreign Affairs' operational scope and associated expenditures, and improve service to the public. The audit found that the use of this digital product is minimal relative to the overall volume of apostille issuance: only a few thousand compared to hundreds of thousands of manual apostille certificates. The Ministry of Justice, with the assistance of the Ministry of Foreign Affairs, should improve the accessibility of this digital product and continue to work to remove existing barriers in some countries that are parties to the Convention, in order to implement the Government decision on this matter, thereby substantially improving public service and reducing state costs associated with manual issuance.

The findings of this report reflect years of neglect in the field of apostilles – in the implementation of the Convention, adherence to financial processes, and service to the public. The Director General of the Ministry, the Deputy Director General for Consular Affairs, and the Head of the Apostille Department should thoroughly examine the deficiencies identified, consider the alternatives and recommendations presented, and – taking a forward-looking perspective and in light of the steadily increasing demand for this service – advance a comprehensive reform of document authentication services and address all identified deficiencies. At the same time as addressing the deficiencies detailed in this report, and until the digital apostille is widely adopted, the Ministry of Foreign Affairs should conduct a strategic assessment, in cooperation with the National Digital Agency and the Ministry of Justice, to realistically evaluate the timeline for the effective implementation of the Government decision on the digital apostille and its expected applicability to the majority of apostille certificates, including its acceptance by most countries that are parties to the Convention.

The Ministry of Foreign Affairs should act in cooperation with the Ministry of Justice and the National Digital Agency to establish a centralized digital process based on the Government Data Exchange Infrastructure and in line with the "once-only" principle. This would provide efficient and high-quality service to applicants in accordance with the Apostille Convention and enable government bodies that issue key documents (such as the Population and Immigration Authority and the Israel Police) to issue apostille certificates for documents they produce. An interim solution is required, in view of the fact that demand for apostille services has been steadily increasing in recent years and has reached hundreds of thousands of requests annually.