Public Prosecution Service of Canada | Service des poursuites pénales du Canada

AUDIT OF THE ELECTRONIC AUTHORIZATION AND AUTHENTICATION PROCESS

FINAL AUDIT REPORT

JANUARY 2022

Internal Audit and Evaluation Division

Canada

As recommended by the Departmental Audit Committee, subject to approval by the Director of Public Prosecutions, on March 29, 2021.

Approved by the Director of Public Prosecutions on January 11, 2022.

Cette publication est également disponible en français.

This publication is available in HTML formats on the Internet at http://www.ppsc-sppc.gc.ca/eng/

Cat. No. J79-12/2022E-PDF
ISBN: 978-0-660-41846-9

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

1.1 OBJECTIVES AND SCOPE

The objective of this audit was to assess the Public Prosecution Service of Canada's (PPSC) Electronic Authorization and Authentication (EAA) process and provide assurance the established controls met the requirements of the Treasury Board of Canada (TB) and the *Financial Administration Act* (FAA).

The audit focused on the application and validation process of electronic signatures on documentation requiring sections 32, 34, and/or 41 of the FAA approvals within the PPSC from March 18, 2020 to August 31, 2020.

The planning and examination phases of the audit were conducted between August and November 2020.

1.2 AUDIT CONCLUSION

The Internal Audit and Evaluation Division (IAED) examined the process and controls for EAA against pre-established criteria based on TB policies, directives and guidance, PPSC policies, directives, and procedures, as well as general best practices.

Overall, there was appropriate governance over the EAA process; however, there were some inconsistencies between documents created to support the new process. These inconsistences lead to discrepancies in some of the data reviewed.

Improvements should be made to the documentation to ensure consistency in the application of electronic signatures. Additional communication and training for employees could further improve overall efficiencies and compliance.

1.3 SUMMARY OF RECOMMENDATIONS

The IAED found that the Finance and Acquisitions Division (FAD) was able to roll out the process in a timely manner considering the sudden need for an electronic signature tool for use by a remote workforce due to COVID-19. It was also found that tools and options for more flexible use of the electronic signature were made available as needs arose, such as how to create multi-signature forms and locking documents after signature. The process was also found to be more efficient for most employees who exercise FAA section 32, 34, and/or 41 signatures routinely.

The report contains the following recommendations:

- The Chief Financial Officer (CFO), in coordination with the Chief Information Officer (CIO), should:
    - Ensure Directives, Standards, and Procedures are cohesive, communicated to employees, and that further training is made available.
    - Ensure that expectations and requirements for verifying signature validity are documented and communicated to employees.

1.4 STATEMENT OF ASSURANCE

In my professional judgment as the PPSC's Chief Audit and Evaluation Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The audit findings and conclusion are based on a comparison of the conditions, as they existed at the time of the audit, against pre-established and approved audit criteria that were agreed upon with the PPSC's management. The findings and conclusion are applicable only to the entity examined. The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada.

I appreciate the cooperation and assistance provided to the audit team by PPSC staff in Headquarters and regional offices.

Cathy Rodrigue
Chief Audit and Evaluation Executive

_____

2.0 INTRODUCTION

2.1 BACKGROUND

The use of electronic signatures is part of the Digital Government initiative, which aims to streamline the Government of Canada's internal and external business processes as well as improve how it delivers services to Canadians. In keeping with this, the Treasury Board of Canada Secretariat issued the Government of Canada Guidance on Using Electronic Signatures. Using an electronic signature meets the aims by replacing paper-based processes with electronic practices that are more modern, faster, and easier to use. The use of an electronic signature meets the fundamental purpose of the signature in that it links a person to a document or transaction and typically provides evidence of that person's intent to approve or to be legally bound by its contents.

At the PPSC, the CFO, along with the Information Technology (IT) group, sought to implement electronic signatures and to move away from the paper-based system of signatures, reviews, and approvals.

After extensive testing, the Information Solutions Branch at the PPSC deployed the use of Foxit Phantom PDF to all PPSC employees as a new software tool that also provides secure signature capabilities.

In March 2020, due to the COVID-19 pandemic, employees were required to work from home for the unforeseeable future. Subsequently, on March 18, 2020, the CFO published a Bulletin on iNet authorizing the use of electronic signatures. The FAD developed and communicated the Standard on Electronic Authorization and Authentication on iNet. This Standard establishes the procedure for the Department to use EAA in lieu of paper-based signatures under the Delegation of Spending and Financial Signing Authorities.

The Standard on EAA directs users to electronically sign documents using Foxit. This signature is assured by having the employee sign into their myKey, which is an encrypted digital key built by the Entrust software, an internal credential management service that facilitates authentication for secure access to applications and Government of Canada networks.

The IAED conducted this Audit of the Electronic Authorization and Authentication Process in accordance with the PPSC's 2020-2021 to 2021-2022 Risk-based Audit Plan, approved by the Director of Public Prosecutions on April 9, 2020.

2.2 OBJECTIVES AND SCOPE

The objective of this audit was to assess the EAA process and provide assurance the established controls met TB and FAA requirements.

The audit focused on the application and validation process of electronic signatures on documentation requiring sections 32, 34, and/or 41 approvals within the PPSC from March 18 to August 31, 2020. Excluded from the audit scope were Agent Affairs transactions as these have their own approval process and have been subject to previous audit review.

The planning and examination phases of the audit were conducted between August and November 2020.

2.3 METHODOLOGY

The audit complied with accepted auditing practices and was conducted in accordance with the TB Policy on Internal Audit.

The audit methodology included:

- interviews with employees in FAD, process stakeholders, and Business Coordinators (BC) in various areas
- review of files and invoices
- a review and analysis of data, documented policies, practices, procedures, and directives.

3.0 FINDINGS

3.1 GOVERNANCE AND COMPLIANCE

There was appropriate governance over the development and implementation of the electronic signature process through approvals and stakeholder engagement. There were no significant compliance issues with TB requirements. While there were issues with long-term validation, these were outside of the PPSC's control and mitigating measures will be put in place.

We expected to find appropriate governance for the EAA process, as well as compliance with TB requirements.

We found that the Standard on EAA was implemented, approved and communicated to employees by the CFO, via bulletin, on March 18, 2020 as per the PPSC Framework on Financial Policy Instruments (Framework). A draft Directive on Electronic Authorization and Authentication of Financial Transactions was in development during this audit and is pending approval as per the Framework. We found that the IT group was consulted concerning TB requirements, assurance level and functionalities for the Foxit software in the development of the Standard and draft Directive.

We found no significant compliance issues with the various TB requirements for electronic signatures. These included:

- Directive on Delegation of Spending and Financial Authorities
- Directive on Identity Management – Annex A: Standard on Identity and Credential Assurance
- Guide to Delegating and Applying Spending and Financial Authorities
- Government of Canada Guidance On Using Electronic Signatures
- Guideline on Defining Authentication Requirements
- Guideline on Identity Assurance
- User Authentication Guidance for Information Technology Systems (ITSP.30.3031.V3)

However, we did find that the current version of Entrust, rolled out across the Government of Canada, has a certificate expiry of five years; this does not meet the seven-year retention period required for financial documents. While this is out of the PPSC's control, some mitigating measures will be implemented once PPSC documentation has migrated to GCdocs, such as keeping documents for the full seven-year period. As GCdocs has an inherent tracking mechanism, an audit trail of any changes will be tracked ensuring the integrity of the document for the duration of the retention period.

The PPSC's Chief Information Officer (CIO) was consulted to determine if Foxit, in conjunction with Entrust myKey, met the assurance level 3 of the Government of Canada Guidance on Using Electronic Signatures. The CIO, upon review, agreed this assurance level was met and the audit team found no compliance issues with this assurance level.

While there is no documentation in place to address any issues or further changes to the EAA process, we found there to be a documented plan to review EAA through ongoing internal controls testing in FAD.

3.2 DOCUMENTATION

Generally, the breadth of documentation and information produced for this new process was appropriate however, inconsistencies were found between the procedures and the Standard on EAA that render it challenging for individuals to apply the correct procedures.

We expected that appropriate and sufficient documentation for electronic signatures was created and communicated to employees.

Generally, expectations for electronic signatures were documented and communicated to employees; however, we found inconsistencies between the procedures listed in Annex A of the Standard on EAA and the supplemental procedures posted on the Information Management Hub on iNet. The supplemental procedures provided further, detailed, directions on inserting electronic signatures in Foxit using 'place' versus 'certify' signature, applying and creating multiple signatures, locking documents, and verifying the validity of signatures. We found, based on interviews with BCs, these procedures were not sufficiently communicated to employees and that some were not aware they existed. Some recurring issues noted by employees, such as documents locking and the inability to insert multiple signatures, were consistent with the variances found in the documentation.

We found the requirements and expectations regarding the verification of a signature's validity were not clear. We found that neither the Standard nor the draft Directive documented these expectations. In addition, there was no internal documentation in FAD regarding the verification of signature validity being part of the process to authenticate the identity and signature in documents when they are received for payment processing. Also, the current documentation did not provide sufficient information on certificate authority nor provide any direction on how to proceed when the validation of an electronic signature comes up as "Unknown".

Improvements could be made to the procedures and the Standard to ensure clarity and a proper workflow for applying signatures in documents, as well as the verification of the validity of signatures.

Recommendation:

The CFO should ensure that Directives, Standards, and Procedures are cohesive, communicated to employees, and that further training is made available. Efforts should be coordinated with the Administrative Services Division for the technical training and alignment with written materials.

3.3 SYSTEM AND INFORMATION INTEGRITY

The current process and behaviours of employees does not always ensure system and information integrity. Not all electronic signatures reviewed were authorized and valid. Incorrect security procedures by employees could put the system at risk.

We expected that electronic signatures for transactions pursuant to sections 32, 34, and 41 of the FAA be authorized, valid and secure.

Human Resources

We reviewed a sample of Letters of Offer and Letters of Change and found a high occurrence of wet signatures during the scope of the audit. The audit team made the decision to review the samples for trends in the use of electronic signatures and potential efficiency gains. We found that there was a spike in the use of electronic signatures in June and July and that wet signatures were consistently used during the audit scope. In addition, the Human Resources (HR) group started verifying signature validity in September, when feasible, given that most documents are returned to HR scanned.

The use of electronic signatures has, in some cases, created more efficiencies in that there is less printing and scanning. Ensuring that candidates and managers are aware they can sign documents electronically would allow the review of the validity once submitted to HR.

Acquisitions

We reviewed a sample contracts to verify electronic signature authority and validity. We found many signatures could not be validated due to the file being scanned, the signature validity and certificate being "unknown", the signature being "invalid" due to changes being made after signature, and one due to having images inserted of the signature box rather than inserted as per the process. The Chief Procurement Officer indicated that there is currently no signature review process in place to verify validity, which could have been beneficial in reducing these occurrences.

Finance

We found through interviews with FAD employees that there is an internal process and checklist for the verification of signatures on invoices to ensure they are from a delegated authority and that the signature matches that of the signee. This process requires verification against an employee's Specimen Signature Record (SSR) that details their level of financial approval authority. With the transition to electronic signatures, we found that FAD created a tracking list of cancelled invoices to note any invoices found to have an issue with the electronic signature, and that these invoices are sent back to the signee for correction.

We reviewed a sample of invoices to verify electronic signature authority and validity. We found occurrences where the electronic signature could not be validated as they were "unknown". It was noted that the signees had used a "@justice.gc.ca" email address and that this could be due to the PPSC sharing a VPN with the Justice Department. However, an interview with a Finance employee confirmed there is an electronic signature validity verification being done, and so these cases should have been corrected.

We also found an invoice where the signee did not have an active delegation through the SSR. Their previous SSR expired in February 2020. The verification of delegation authority is an existing process that occurs when processing invoices for payment; this was expected to continue even with EAA as it is not dependent on how the invoice was signed. Non-valid or unauthorized signatures could have an impact on the integrity of the financial transaction being processed and are non-compliant with the FAA.

In both contract and invoices, we found the following discrepancies:

- changes to documents were made after signing;
- text boxes were left open;
- signature fields were left open; and

- signee not using the reason "I am approving this document" as required by the procedure.

We found that BCs in several regions were continuing to have issues with the EAA process. They noted that support from Headquarters regarding the Standard and Procedures was not always timely and that they did not know who to contact to resolve their issues. It was also noted that additional training for the EAA process would be welcome, as previously noted in section 3.2 of this report.

Recommendation:

The CFO should document and communicate expectations and requirements for verifying signature validity to employees. Efforts should be coordinated with the Administrative Services Division for the technical training and alignment with written materials.

4.0 CONCLUSION

The IAED examined the process and controls for EAA against pre-established criteria based on TB policies, directives and guidance, PPSC policies, directives, and procedures, as well as general best practices.

Overall, there was appropriate governance over the EAA process; however, there were some inconsistencies between documents created to support the new process. These inconsistences lead to discrepancies in some of the data reviewed.

Improvements should be made to the documentation to ensure consistency in the application of electronic signatures. Additional communication and training for employees could further improve overall efficiencies and compliance.

5.0 MANAGEMENT ACTION PLAN

RECOMMENDATION	MANAGEMENT RESPONSE AND ACTION PLAN	OFFICE OF PRIMARY INTEREST	TARGET DATE
1. The CFO should ensure that Directives, Standards, and Procedures are cohesive, communicated to employees, and that further training is made available. Efforts should be coordinated with Administrative Services Division for the technical training and alignment with written materials. *Risk: Medium*	FAD will modify the standard while coordinating these efforts with IM/IT for consistency in documentation and support for technical training. Documentation will be available on iNet and training sessions will be organised.	CFO	Q3 – 2021-22
2. The CFO should document and communicate expectations and requirements for verifying signature validity to employees. Efforts should be coordinated with Administrative Services Division for the technical training and alignment with written materials. *Risk: Medium*	FAD will develop a policy instrument that addresses the signature validity requirements and will work collaboratively with IM/IT to offer the appropriate training.	CFO	Q3 – 2021-22

APPENDIX A – AUDIT CRITERIA

Audit Criteria
1. Appropriate governance over the electronic signatures process is in place and functioning.
2. Appropriate and sufficient documentation was created and communicated.
3. The electronic signature authorization and authentication process ensures system and information integrity.
4. Long-term document retention requirements related to electronic authorization and authentication are met.

APPENDIX B - LIST OF ACRONYMS/ABBREVIATIONS

BC	Business Coordinators
CFO	Chief Financial Officer
CIO	Chief Information Officer
EAA	Electronic Authorization and Authentication
FAA	Financial Administration Act
FAD	Finance and Acquisitions Division
HR	Human Resources
IAED	Internal Audit and Evaluation Division
PPSC	Public Prosecution Service of Canada
SSR	Specimen Signature Record
TB	Treasury Board of Canada