SC 1961 APOSTILLE

OCTOBER 2021

PREL. DOC. NO 9

Title	PB Role in Digital Certification
Document	Prel. Doc. No 9 of September 2021
Author	PB
Agenda Item	Item 9.ii.
Mandate(s)	Experts' Group on the e-APP and New Technologies
Objective	To outline possible ways to standardise digital certification in the context of the e-APP and the role of the PB in facilitating this process.
Action to be Taken	For Decision ☐ For Approval ☐ For Discussion ☒ For Action / Completion ☐ For Information ☐
Annexes	N/A
Related Documents	N/A

Table of Contents

PB Role in Digital Certification

I. Introduction

1 The issuance of an e-Apostille requires the use of a digital certificate to validate the signature, making digital certificates an integral part of the e-APP. As with all aspects of the e-APP, Contracting Parties have full discretion regarding the digital certificate infrastructure used by their Competent Authorities. However, the variety of digital certificates used by Contracting Parties has led to misunderstandings in practice and, in some cases, rejections of e-Apostilles.

2 The Experts' Group on the e-APP and New Technologies, which met in May 2021, discussed the potential for standardising e-Apostille issuance and verification. This included consideration of digital certification standards and the possibility of evaluating and accrediting e-APP solutions from commercial providers. While the Group concluded that full harmonisation was neither necessary nor desirable, it acknowledged that further discussion may be required in relation to international standards, licensing, and third-party accreditation.[1]

3 The goal would be to increase uptake of the e-APP by supporting Contracting Parties in the implementation of the e-Apostille component. Specifically, it would assist Contracting Parties who do not have the resources or time to develop internal infrastructure. If more Contracting Parties are issuing e-Apostilles, this would also increase their acceptance. Depending on the model chosen, there may also be an element of revenue generation.

4 Against this background, this document explores possible standardisation of digital certificates under the e-APP and the role that the PB might play in facilitating this process.

II. Digital Certificates and the e-APP

5 Digital certificates are issued by a certificate authority, which is either public or private, using public key infrastructure. Whether a certificate authority is public or private refers to the extent to which other entities trust its certificates and not whether the certificate authority itself is public or private in nature. Certificates from a public certificate authority (*e.g.*, IdenTrust, DigiCert, and GlobalSign) are "publicly trusted" and available for widespread use, as they are recognised by major browsers, applications, and devices.[2] By contrast, certificates from a private certificate authority are designed for use within a group of authorised users or devices (such as within a company or organisation) and may lead to errors or warnings if they are used outside this group. Given the purpose of the Apostille Convention and the many uses of (e-)Apostilles, publicly trusted digital certificates are most appropriate for the e-APP.

6 In some certification structures, there is a hierarchy of multiple certificate authorities. The "root" or "anchor" certificate authority is at the highest level, followed by a "subordinate" or "intermediate" certificate authority to determine permissions at other levels, and then the "issuing" certificate authority at the lowest level, responsible for the actual issuance of the digital certificate. In such a hierarchy, whether a digital certificate is publicly or privately trusted is determined by whether the root certificate authority is public or private.

7 Where a commercial solution from a public certificate authority is not considered appropriate, such as for policy or security reasons, it is possible to create a purpose-built, root certificate authority. However, the development, maintenance, and security costs can be significant, and there is no guarantee that the certificates issued will be able to achieve the same level of public trust that

---

1 See Prel. Doc. No 6 of May 2021, "Report from the Chair on the Experts' Group on the e-APP and New Technologies", Annex I, para. 12.

2 See *e.g.*, current members of the Adobe Approved Trust List (AATL), available at: < https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html >.

existing certificate authorities enjoy. This can lead to difficulties for users and, in the context of the e-APP, increase the risk of rejection of e-Apostilles that rely on these digital certificates.

8 To overcome this difficulty, some public certificate authorities offer "hosting" services, allowing an organisation to manage their own certificates as a subordinate (intermediate) certificate authority. This allows the organisation to retain full control over the issuance of its digital certificates without the cost of establishing its own root certificate authority, ensuring that the organisation's digital certificates fully benefit from the near universal trust of a public certificate authority.

III. A Dedicated Certificate Authority

9 The establishment of a dedicated certificate authority could standardise digital certification under the e-APP. Providing standardised digital certificates to Competent Authorities would reinforce trust among Contracting Parties and facilitate the circulation, verification, and acceptance of e-Apostilles. It would also assist Contracting Parties that have not yet implemented the e-Apostille component,[3] expediting the e-APP implementation timeline by avoiding the need for Contracting Parties to develop an internal digital certification infrastructure. In addition, it could prove more cost-effective for Competent Authorities that would otherwise have independently used solutions from commercial providers.[4]

10 Recognising the importance of implementation flexibility, any digital certification solution would be optional and would have no impact on Contracting Parties employing or developing their own digital certificate solutions for e-Apostilles. In addition, the fact that an e-Apostille uses a digital certificate other than the standardised certificate would not be a valid ground for rejection.

11 If Contracting Parties support the establishment of a dedicated certificate authority, it is important that this work be coordinated centrally, and with the involvement of Competent Authorities. The PB would be best placed to manage this process, ensuring that all current and future Contracting Parties can benefit from any infrastructure developed.

12 Acknowledging the sensitivity of its role as secretariat and the lack of technical expertise, the PB would not develop and maintain its own internal certificate authority. Instead, considering the structures outlined above and the need for certificates that are as widely accepted as possible, the most appropriate and least resource-intensive model would be for the PB to act as a subordinate certificate authority, hosted by a public root certificate authority (as described at para. 8). All interested Contracting Parties could then obtain the necessary credentials for their Competent Authorities from the PB, issuing e-Apostilles using the publicly trusted digital certificates specifically designed for use under the e-APP.

13 In an effort to focus discussion on the desirability of the proposal, the PB has not identified specific technologies to be employed at this time, nor has it included potential costs associated with such work. If there is support for the proposal, the PB would further explore options for development. Any solution developed for this purpose would be appropriate for use in all interested Contracting Parties and may incorporate a mechanism for possible revenue generation, including to recover costs associated with development and maintenance.

---

3 Approximately 20% of Contracting Parties have implemented the e-Apostille component of the e-APP. Most Contracting Parties could therefore benefit from a readily available digital certificate infrastructure. See "Implementation Chart of the e-APP" available on the Apostille Section of the HCCH website at < www.hcch.net >.

4 Based on current trends, a significant number of Contracting Parties would use commercial solutions. From responses to the 2021 Apostille Questionnaire, of those Contracting Parties that currently issue e-Apostilles, approximately 40% use technology from commercial providers. See Prel. Doc. No 2 of August 2021, "Summary of Responses to the Apostille Questionnaire", paras 48 *et seq*.

IV. Proposal for the Special Commission

14 The Special Commission is invited to consider whether the establishment of a dedicated certificate authority for the e-APP is desirable, and if so, to recommend that the PB submit a proposal to CGAP for consideration.