Doc 9303, Part 13
Eighth Edition
Corrigendum No. 1
English only
11/12/20

Machine Readable Travel Documents

Part 13 — Visible Digital Seals

Eight Edition

CORRIGENDUM No. 1

1. Please replace page App A-1 with the following replacement page in Doc 9303, Part 13, Eighth Edition bearing the following notation:

11/12/20
Corr. 1

2. Please record the entry of this Corrigendum on page *(iii)*.

— END —

Appendix A to Part 13

EXEMPLARY USE CASE (INFORMATIVE)

This section gives a general overview of using a digital seal to protect a non-electronic document. The specific use case considered here is the protection of a visa document, and depicted in Figure A.1. Whereas technical details may vary for other use cases, the same general principles apply.

The general workflow can be separated into three steps. As a prerequisite, Visa Signer Certificates (VSCs) have to be generated. Next, digital seals are generated, and then later validated.

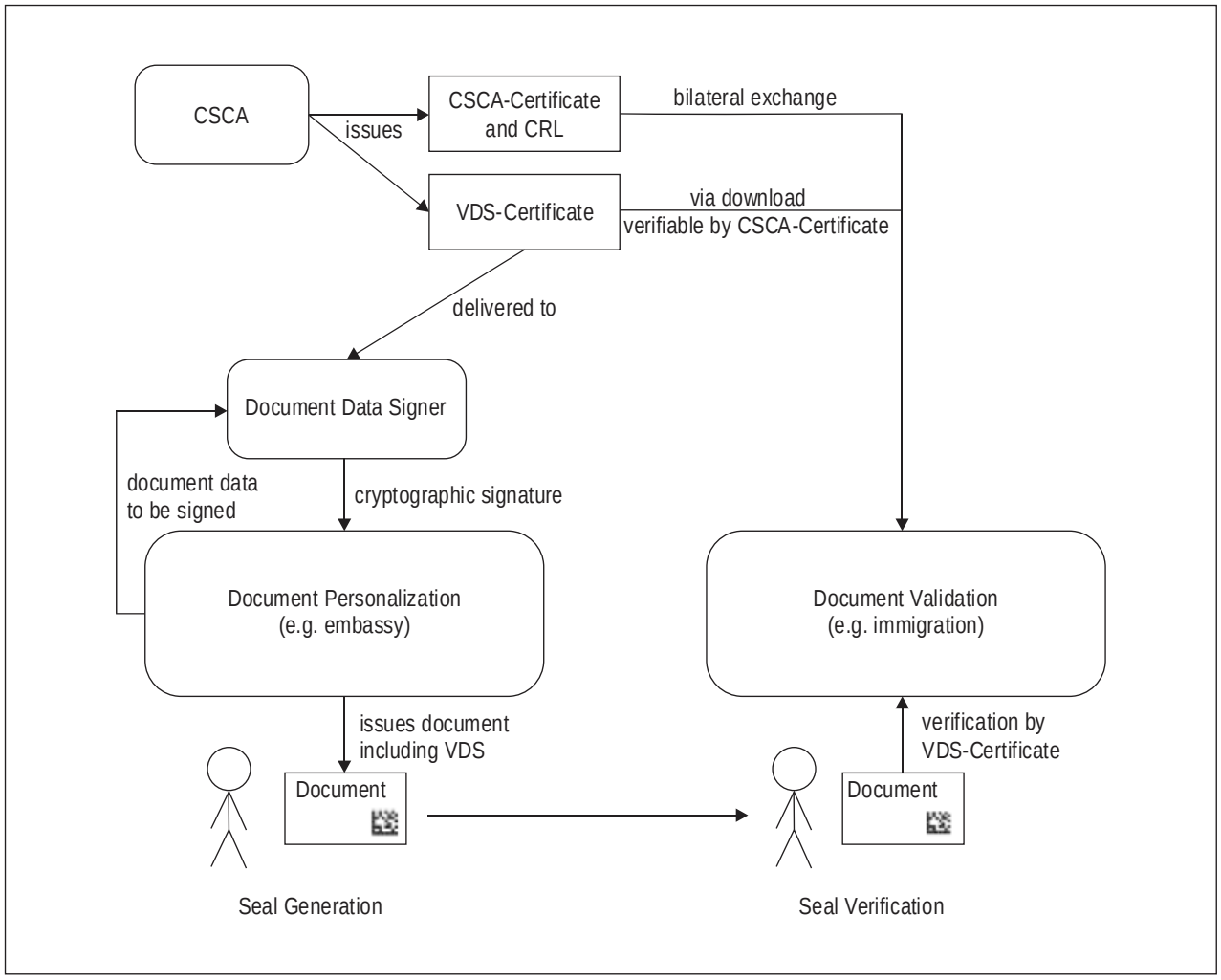

Figure A.1. Exemplary VDS Use Case

A.1 PREREQUISITE: VISA SIGNER CERTIFICATE GENERATION

The visa signing PKI is based upon the PKI set-up for electronic passports defined by ICAO. At the root is the Country Signing Certificate Authority (CSCA) of each country. The CSCA publishes a CSCA-Certificate containing the public key of the CSCA. To enable trust between countries, this CSCA-Certificate is distributed in a trustworthy manner via bilateral exchange, or via master lists.

The Visa Signer is the entity that actually signs digital seals. VSCs are issued by the CSCA and can therefore be verified by the CSCA-Certificate.

A.2 DIGITAL SEAL GENERATION

A digital seal is generated in two steps:

a) Applicants apply for a visa at the embassy where they reside. The embassy records the applicant's data and checks whether the applicant meets the requirements to receive a visa. If the requirements are fulfilled, the embassy sends a digital representation of the recorded data to the Visa Signer (VS). The VS can either be (1) a central entity located in the country that issues the visa, and the embassy connects to the VS via a secure channel, or (2) the VSs are decentralized entities placed at each embassy, for example, using smartcards containing cryptographic keys that are directly attached to the personalization system. In either case, the VS cryptographically signs the recorded data.

b) For signing, the Visa Signer uses a key pair of a private key and a public key. The actual signing is done with the private key, whereas the public key is stored in a Visa Signer Certificate. The resulting signature is sent back to the Visa Personalization System if the Visa Signer is not a local part of the personalization system, printed on the visa sticker and attached to the applicant's passport.

A.3 DIGITAL SEAL VALIDATION

When applicants enter the issuing country, they present their visas to a Visa Validation Authority (VVA), e.g. the immigration control authority of the issuing country. The VVA verifies the authenticity and integrity of the digital seal on the visa by validating the signature of the seal, and comparing the printed information on the visa sticker and on the passport with the digital information stored in the seal. The signature of the seal is verified by identifying the corresponding VS-Certificate with the help of the identifier stored in the header of the digital seal, and then using the public key of the VS-Certificate. As described in the previous paragraphs, the validity of the VS-Certificate itself can be verified by the CSCA-Certificate.

Remark

Since all certificates are publicly available, the validity of the visa can be verified by *any* third party, not just by the issuing State. This approach can thus handle use cases for unions of countries, where one country issues a visa for another country (as is done for example in the European Union). Another use case is verification of visas by airlines prior to boarding a plane.

Remark

The criteria to determine if a visa document can be trusted or not, based on the digital seal and the MRZs of the visa and the passport, are defined in a validation policy.

— — — — — — — —