September 10, 2026

Visible Digital Seal (VDS)

Implementation Guidelines 2026

Draft Version 0.1

Office of the Controller of Certifying Authorities (CCA)
Information and Communication Technology (ICT) Division

Document Control

Document Title	Visible Digital Seal (VDS) Implementation Guideline
Document Status	Draft
Version	0.1
Approval Date	
Published Date	
Document Issuer	Office of the CCA
Approver	….. …..
Signature	

Table of Contents

Document Control 1
1. Introduction 4
1.1. Purpose 4
1.2. Objectives 4
1.3. Scope 4
2. VDS encoding and formatting standards 5
2.1. MRC Representation 5
2.2. Data Interchange Format 5
2.3. Language & Characters 5
2.4. Date & Time 6
2.5. Canonicalization 6
2.6. Payload Envelop Structure 6
2.6.1. Data Zone 6
2.6.2. Signature Zone 7
2.6.3. Payload sample structure 7
2.6.4. Basic requirements 7
3. Signature Semantics 8
3.1. Signature Creation 8
3.2. Signature Verification 8
3.3. Signature Technical Specification 9
3.4. e-Seal Private Key Protection 9
4. PKI and VDS Certificate Profile 9
4.1. e-Seal Certificate 9
4.2. Certificate validation 9
4.3. CRL distribution and revocation 10
4.4. Validity periods 10
4.5. Offline verification 10
5. National trust and profile-authorization registry 10
5.1. Trust model 10
5.2. Organization identity and authorization 10
5.3. Registry specification 11
6. National Document Profile for VDS 11
6.1. Identifier and ownership 11
6.2. Profile Contents 11
6.3. Versioning 11

6.4. Registration and publication 12
7. Roles and responsibilities 12
7.1. Controller of Certifying Authorities 12
7.2. Certificate Authorities 12
7.3. Document Issuer Authority 12
7.4. VDS Solution Provider 12
7.5. Verification solution provider 13
7.6. Relying party and document holder 13

1. Introduction

1.1. Purpose

A Visible Digital Seal (VDS) is a secure, cryptographically signed machine readable code (MRC) represented into electronic or physical documents to verify their authenticity. In most cases 2D barcode, such as QR code are applied to physical or digital documents as MRC. Credential issuers in government and private sectors can use VDS into their issued document to ensure authenticity and integrity of the document and the data within the document. This technology supports reliable verification of printed and digital documents through a MRC printed in the document. The purpose of this guideline is to establishes a national framework and associated standards for ensuring interoperability and uniformity among participants (issuer, holder, trust service provider, and relying parties) of VDS technology.

1.2. Objectives

The objectives of this guideline is to:

a) Establish a consistent national approach for issuing and verifying VDS documents in Bangladesh;
b) Enable reliable verification of documents presented in printed or digital form;
c) Provide integrity and signer-authentication assurance for structured document data in physical world;
d) Support Bangla and English without changing signed data during verification;
e) Support documents that may remain valid after the signing certificate expires;
f) Assign clear responsibilities to CCA, Certification Authorities, profile owners, issuers, verifier providers and relying parties.

1.3. Scope

This guideline shall be applied for VDS implementations in Bangladesh and may differ from VDS related international standards in few areas according to the necessity of the country context. The application area of VDS is for any printed or electronic documents which is listed under approved document profile published by the Office of the CCA. The guideline is not applicable for any document which is governed by any international body or international profile (such as travel document is governed by ICAO Doc 9303 Profiles).

A valid VDS authenticates the signed data zone and may be copied together with its signed content. Relying parties shall therefore compare verified data with the visible document and perform any separate identity, entitlement or physical-document checks required by law or business policy. Identity authentication of the person presenting the document is not within the scope of the VDS technology. The VDS will only ensure the Identity authentication of the organization from where it has been issued using digital seal/e-Seal.

The guideline governs the payload envelope, language declaration, canonicalization, signature, certificate handling, PKI validation, profile authorization, MRC baseline, verification sequence, result semantics and governance whereas each national document profile governs its document categories, issuers, language-specific message keys, field definitions, identifiers, date and expiry rules, document status, retention and sector-specific controls.

2. VDS encoding and formatting standards

2.1. MRC Representation

Various categories of QR codes and other 2D barcode representations, such as DataMatrix and Aztec, are allowed to ensure global interoperability, and VDS readers should be capable of reading all types. The QR Code shall carry the complete JSON payload, where UTF-8 encoding is one option among others to support global interoperability.

The QR Code shall be printed or displayed as a geometrically square symbol with a quiet zone of at least four modules on every side. It shall have sufficient contrast and module definition for reliable capture. Scaling is left to the discretion of the users to ensure usability and adoption; smoothing, resampling and decorative alteration of modules are prohibited. QR configuration shall set the final module dimension and ISO/IEC 15415 print-quality threshold. Issuers are encouraged to test representative production samples where possible, but this is not a mandatory requirement for document issuance.

2.2. Data Interchange Format

It is very essential to maintain a common data format to be used by the involved information systems within the VDS technology ecosystem. The VDS payload shall be a single JSON object; while UTF-8 is recommended, other encodings are permitted to ensure interoperability. Adherence to I-JSON constraints in RFC 7493 (such as prohibiting duplicate member names) is encouraged to maximize interoperability, though issuers are permitted flexibility in payload structure to accommodate their specific data requirements alongside the restrictions in this guideline and the selected National Document Profile. Some key characteristics of the JSON format are:

a) JSON member names shall be unique within an object; duplicate member names shall be rejected.
b) Numbers shall be within the interoperable I-JSON range and shall not use NaN or infinity.
c) The payload shall contain The payload shall contain valid UTF-8 text; other encodings may be used as an option. Invalid UTF-8 sequences and JSON Unicode escapes that do not represent valid Unicode characters shall be rejected.
d) The outer structure and each profile schema shall reject unspecified members unless an explicit extension point is defined.
e) Implementations shall impose profile-defined limits on bytes, nesting depth, strings, arrays and member counts before full parsing.

2.3. Language & Characters

Each signed payload shall contain human-readable data in one declared language only. The Header member named “ln” shall be either ‘bn’ for Bangla or ‘en’ for English. Bangla and English human-readable values shall not be mixed within the same signed payload. Language-neutral identifiers, codes, dates and cryptographic values shall remain in ASCII for both languages.

Where the same document is issued in separate Bangla and English versions, both payloads shall contain the same document identifier and identical language-neutral data. The applicable National Document Profile shall declare which language version is authoritative if the language versions conflict.

For Bangla (i.e. when “ln” is “bn”), selected human-readable “msg” member names and their human-readable string values shall be expressed in Bangla as defined by the Bangla JSON Schema for the profile. Structural, Header and Signature member names shall remain the fixed ASCII names defined

by this Guideline. Identifier fields, code values, dates and other language-neutral values shall remain in the syntax defined by the profile. Members containing Bangla values shall use Unicode encoded directly in UTF-8 whether the member name shall be always English. The issuer shall normalize Bangla member human-readable values to Unicode Normalization Form C (NFC) before schema validation and signing. Legacy non Unicode encoded text shall not appear in a signed payload. A verifier shall preserve the received Unicode strings and shall use a font, preferably BCC Purno (a.k.a July) font or Nikosh font and the shaping engine shall be capable of displaying Bangla conjuncts correctly.

Government may publish a separate Bangla Text Handling Specification covering ZWJ/ZWNJ, whitespace, punctuation, digits, conversion quality and reference test cases.

2.4. Date & Time

A date or timestamp included in a payload shall use the format prescribed by its National Document Profile. A time-bound profile shall also define a signed expiry field. A profile for a document with no natural expiry may prohibit or omit the expiry field; the profile registry shall state that the document is non-expiring unless cancelled or superseded. The profile shall use “iat” and “exp” as defined in RFC 8392.

2.5. Canonicalization

Before signing, the issuer shall apply the JSON Canonicalization Scheme (JCS) as defined in RFC 8785 to the complete data object. The canonical representation shall then be encoded as UTF-8 (recommended; other encodings permitted for interoperability) and supplied to the signing operation.

2.6. Payload Envelope Structure

VDS payload shall be a single JSON object; while UTF-8 is recommended, other encodings are permitted to ensure interoperability. The complete JSON object shall be encoded in the QR Code without additional text, prefixes or transport wrappers unless expressly specified by this Guideline.

The payload shall contain exactly two top-level members:

- Data zone represented as “data”, containing the document information protected by the digital signature; and
- Signature zone represented as “sig”, containing the information required to verify that signature.

2.6.1. Data Zone

Data zone consists of two part, the header and the message. The header (hdr) object shall contain the following four members and no others:

Header		
Member	Type	Requirement
t	string	Registered National Document Profile identifier in the form bd.<functional_area>.<profile>
v	integer	Positive profile version number identifying one immutable published schema set.
is	string	(Optional) Short form of organization ID if available
ln	string	Declared language: bn or en.

The combination (t, v, ln) shall resolve to exactly one authenticated profile package in the official CCA repository. A verifier shall not guess an unknown profile, version or language.

The message (msg) object contains the signed document data. The permitted keys, language-specific key mapping, values, types, mandatory status, maximum lengths, identifiers, code tables and cross-field constraints shall be defined exclusively by the selected profile schema. Every profile shall define a stable document-identifier semantic field and an issuance-date or issuance-timestamp semantic field.

2.6.2. Signature Zone

The signature (sig) object shall contain the following three members and no others:

The signature (sig) object shall contain the following four members: alg, sigvl, and the full certificate (cer) and its serial number (ser).

Member	Type	Requirement
alg	string	Fixed value ES256 (ECDSA P-256)
cer	string	Complete DER-encoded organizational e-seal certificate (encoded as unpadded base64url).
ser	string	Certificate serial number.
sigvl	string	Raw fixed-width ECDSA signature, encoded as unpadded base64url.

2.6.3. Payload sample structure

Example structure of payload:

```
{
 "data": {
  "hdr": {
   "t": "bd.<profile>",
   "v": 1,
   "is": <short_form_of_org_id>,
   "ln": "bn"
  },
  "msg": {
   "<key1>": "<values>",
```

```
    "<key2>": "<values>"
   }
  },
  "sig": {
   "alg": "ES256",
   "cer": "<base64url-encoded certificate>",
   "ser": "<certificate-serial-number>" (Optional, one or the other),
   "sigvl": "<base64url-encoded signature>"
  }
 }
```

2.6.4. Basic requirements

The following requirements shall apply:

a) Data and Signature shall each occur exactly once and shall contain JSON objects.
b) Duplicate member names shall be rejected at every level.
c) Additional top-level members shall not be permitted.
d) A missing, empty or incorrectly typed data or signature member shall cause the payload to be rejected.
e) The payload shall comply with the size, nesting and resource limits specified by this Guideline, the national QR configuration and the applicable National Document Profile.
f) A verifier shall treat all decoded payload content as untrusted until the signature, certificate path and applicable authorization checks have been completed.
g) A verifier shall not display decoded values as verified information merely because the QR Code was successfully read.

3. Signature Semantics

The complete data object part of the VDS payload shall be cryptographically signed. The sig object is not part of the signed input.

3.1. Signature Creation

The signature shall protect the complete data object, including header and message. The signer shall:

a) Construct data and validate it against the common schema and the applicable National Document Profile selected by (t, v, is, ln).
b) Confirm that the language rules are satisfied, all applicable text is in NFC, and the JSON contains no duplicate member names.
c) Canonicalize data in accordance with RFC 8785 and encode it as UTF-8 (recommended; other encodings permitted for interoperability):

    signatureInput = UTF8(JCS(data))

d) Sign signatureInput using ES256.

e) Serialize the resulting r and s values as unsigned, fixed-width, 32-octet, big-endian integers and concatenate them as r || s. The result shall be exactly 64 octets. Low-S normalization is not required.
f) Encode the 64-octet signature as unpadded Base64url and place it in sigvl.
g) Create the Signature Zone containing:

alg, with the fixed value "ES256";
cer, containing the base64url-encoded organizational e-seal certificate;
ser, containing the certificate serial number; and
sigvl, containing the encoded signature.

h) Add sig to the same data object used to create the signature. data shall not be modified or regenerated after signing.
i) Apply standard canonicalization (JCS) to the complete payload object and encode as UTF-8 (recommended; other encodings permitted for interoperability):

qrBytes = UTF8(JCS(payload))

j) Confirm that canonicalizing data from the completed payload produces exactly the same signatureInput bytes used for signing. If it does not, issuance shall fail.
k) Encode qrBytes in the approved QR Code configuration.

3.2. Signature Verification

At the relying party end, the verifier shall follow the below steps:

a) Decode the QR Code, decode its contents as UTF-8 and parse the JSON. Malformed UTF-8, malformed JSON and duplicate member names shall be rejected.
b) The verifier shall apply JCS (RFC 8785) to the data object to produce the canonical form. This canonical form shall be encoded using UTF-8 (recommended; other encodings permitted for interoperability) to produce the signatureInput bytes for signature verification. The complete VDS-NC JSON object need not be canonicalized.
c) Validate data against the common schema and the National Document Profile selected by (t, v, is, ln). Confirm that the declared language rules are satisfied and applicable text is already in NFC.
d) Confirm that alg is exactly "ES256" and decode cer as a valid organizational e-seal certificate containing the corresponding public key.
e) Decode sigvl as unpadded Base64url. The result shall be exactly 64 octets. Split it into the 32-octet r and s values and confirm that both are within the valid P-256 range. Low-S normalization is not required.
f) Verify the ES256 signature over signatureInput using the public key contained in cer.
g) Validate the certificate chain, certificate policy, Key Usage, validity and CRL status under the Bangladesh PKI trust framework.

3.3. Signature Technical Specification

Following signature stack is permitted in the for the VDS implementation, any changes due to deprecation of algorithm or standards requires a later approved revision of the guideline and coordinated rollover under the Bangladesh PKI regulation.

Parameter	Requirement
Algorithm identifier	ES256

Parameter	Requirement
Signature algorithm	ECDSA
Hash	SHA-256
Curve	NIST P-256
Signature encoding	Raw 64-octet r || s (32 octets each, unsigned big-endian); not ASN.1 DER
Text encoding	Unpadded base64url

3.4. e-Seal Private Key Protection

The organizational e-seal private key shall be generated, stored and used according to the guideline of CCA. Any additional VDS specific controls published by CCA shall apply. The signing service shall enforce authorized profile use, validated input, certificate status, auditable requests and separation between application data and private-key operations.

4. PKI and VDS Certificate Profile

4.1. e-Seal Certificate

The barcode signer shall use an organizational e-seal certificate issued under the Bangladesh PKI. The certificate public key shall be P-256 and shall support ES256. A certificate using another key type or curve shall not be used for current release of VDS.

The certificate and its serial number shall be included in every payload as defined in the signature zone. Its naming, identity proofing, certificate policy, Key Usage, validity and extensions shall follow the applicable organizational e-seal certificate profile according to the interoperability guideline. The certificate shall unambiguously identify or link to the organization uniquely.

4.2. Certificate validation

A verifier shall build and validate the certificate path to an approved Bangladesh trust anchor. It shall validate certificate signatures, basic constraints, path constraints, Key Usage, certificate policy, naming rules, validity period and revocation status in accordance with the applicable CCA PKI policy.

If only the certificate serial number is present, the verifier shall fetch the corresponding certificate from the authorized certificate repository prior to path validation.

A signature result shall not be reported as VERIFIED unless the embedded certificate has an acceptable path, the issuing CA is trusted, revocation status is acceptable and the signer organization is authorized for the declared profile.

4.3. CRL distribution and revocation

Certificate revocation shall be determined using Certificate Revocation Lists (CRLs) published under each respective CA. The certificate shall contain or resolve to the applicable CRL distribution information in accordance with the CCA's PKI interoperability guideline and CA's Certificate practice statement. OCSP check is not required by this Guideline.

4.4. Validity periods

CA and organizational e-seal certificate validity periods shall be those defined by the applicable CCA PKI Interoperability Guideline Policy and Certification Practice Statements.

Document validity is independent of certificate validity. A profile may define a finite lifetime or may state that the document has no natural expiry. The CCA profile registry shall publish that rule. Expiration of the signing certificate shall not automatically invalidate a previously issued document where acceptable historical issuance and revocation evidence demonstrates that the document was issued while the certificate and authorization were acceptable. If a document was signed when the certificate was valid and not revoked- the signature shall be considered valid, during that signing time.

4.5. Offline verification

Offline software may verify payload syntax and the mathematical signature using the embedded certificate. It may report cached certificate, CRL, authorization and profile information only while each item remains within its approved freshness period. If a required online or historical check cannot be completed, the final result shall be INDETERMINATE and shall identify the checks that succeeded and those that were not performed

5. National trust and profile-authorization registry

5.1. Trust model

Trust in a Bangladesh VDS implementation shall be established through three coordinated mechanisms:

a) The general-purpose national PKI Trust List published by CCA;
b) Validation of the organizational e-seal certificate embedded in the VDS payload; and
c) The CCA profile-authorization registry.

The national PKI Trust List establishes which Certificate Authorities and trust anchors are recognized in Bangladesh. Certificate-path validation establishes whether the embedded organizational e-seal certificate was issued under a trusted certification path. The profile-authorization registry establishes whether the identified organization was authorized to issue documents under the declared National Document Profile.

Successful signature verification alone shall not establish a trusted VDS result. A verifier shall also validate the certificate path, certificate status and profile authorization applicable at the relevant issuance time.

5.2. Organization identity and authorization

The issuing Certificate Authority shall verify the identity of an organization in accordance with the applicable CCA policies and the CA's approved Certification Practice Statement. The CA shall issue the organizational e-seal certificate and bind it to an organization identifier recognized under the national PKI framework. The responsible sector authority shall determine whether the organization is eligible to issue documents under a particular National Document Profile.

CCA shall approve or register the resulting profile authorization and maintain the authoritative association between:

a) The organization identifier;
b) The profiles the organization is permitted to issue;
c) The effective period and status of each authorization.

Issuance of an organizational e-seal certificate by a CA shall not, by itself, authorize the organization to issue a VDS document profile. Certificate renewal, replacement or rollover shall not create a new organizational identity or automatically change the organizations' profile authorizations.

5.3. Registry specification

The machine-readable format, signing method, API or file schema, discovery mechanism and interoperability requirements for the profile-authorization registry are outside the scope of this Guideline. They shall be defined by the Office of the CCA.

6. National Document Profile for VDS

6.1. Identifier and ownership

Every document family shall be defined by a National Document Profile with a lowercase ASCII identifier in the form bd.<profile>. A responsible ministry, regulator or public authority shall submit the profile to CCA. The sector authority owns the profile's business meaning, legal basis, issuer eligibility, fields and lifecycle. CCA approves the technical, cryptographic, PKI, trust and interoperability aspects and registers the profile.

6.2. Profile Contents

Each profile version shall publish separate machine-readable JSON Schemas for ln = bn and ln = en. Both schemas shall represent the same semantic document model but may use different selected human-readable msg member names. The common structural, Header and Signature schemas remain controlled by this Guideline. The language schemas shall reject unspecified members unless the profile defines an extension point. Issuers and verifiers shall select the exact schema using (t, v, ln) and shall not infer a language from the characters present. Profile shall contain following information during submission to the CCA:

a) Profile title, identifier, version, status, owner, approval date;
b) Covered document categories and legal basis;
c) Eligible issuers and evidence required for CCA authorization;
d) Issuance date or timestamp, and any expiry field;
e) Data types, required status, maximum lengths, nesting levels, patterns, and cross-field rules.

6.3. Versioning

A published profile version and its schemas shall not change silently. A publication defect that does not alter semantics may be corrected through a documented erratum. A new required field, changed interpretation, changed key mapping, widened issuer eligibility or incompatible constraint shall require a new profile version. Old profile versions and schemas shall remain available for the document verification horizon.

6.4. Registration and publication

a) The sector authority submits the profile proposal, legal basis, issuer population assessment to CCA.
b) CCA coordinates technical, cryptographic, PKI, trust, privacy and interoperability review.
c) CCA assigns the bd.<profile> identifier and approves the initial version.
d) CCA publishes the profile metadata and discovery information in the official repository; the profile owner publishes or supplies the approved schemas and code tables through that controlled channel.
e) CCA authorizes each organization for the profile .

f) Changes, deprecation and retirement are registered with effective dates while historical verification support is preserved.

7. Roles and responsibilities

7.1. Controller of Certifying Authorities

a) Own, approve and maintain this Guideline and the national document profile registry;
b) Approve National Document Profiles for technical, PKI, trust and interoperability compliance;
c) Govern the national PKI trust anchors and applicable e-seal policies;
d) Maintain and publish the official profile repository, along with versioning and discovery information, authoritative endpoint;
e) Coordinate emergency withdrawal, incident notices and controlled restoration.

7.2. Certificate Authorities

a) Issue and manage organizational e-seal certificates under approved CCA guidelines;
b) Ensure compliance with this guideline for technical specifications regarding VDS;
c) Publish current and historical CRLs with integrity, availability and emergency-update capability;
d) Notify CCA and affected organizations of compromise, revocation or material certificate error.

7.3. Document Issuer Authority

a) Define the document's legal and business meaning, eligible issuers and data requirements;
b) Submit versions and changes to CCA for registration and approval.
c) Maintain active CCA authorization for each profile it signs;
d) Protect its organizational e-seal key and signing service under the CCA policy;
e) Validate source data, language, schema and QR configuration before issuance;
f) Preserve audit and historical evidence for the applicable areas
g) Correct, replace or cancel documents and publish status changes where required by the profile.

7.4. VDS Solution Provider

The VDS Solution Provider shall:

a) Implement the encoding, canonicalization, signature, certificate and QR Code requirements of this Guideline.
b) Support only CCA-approved document profiles and validate every payload against the applicable (t, v, ln) schema before signing.
c) Generate ES256 signatures using the issuer’s organizational e-seal certificate and protect the private key.
d) Prevent signing with an invalid certificate or by an organization that is not authorized for the declared document profile.
e) Generate QR Codes that comply with the approved national configuration.
f) Maintain audit records containing the issuer, profile, certificate reference, signing time, result and hash of the canonical data object. Full personal-data payloads should not be included in audit logs.

7.5. Verification solution provider

a) Implement safe parsing, ES256 verification, PKI validation, CRL checks and profile validation;
b) Use authenticated CCA profile, authorization and discovery information;
c) Enforce freshness, rollback protection and structured offline outcomes;

d) Render Bangla correctly and clearly separate verified from unverified data;
e) Retain enough technical evidence for audit without excessive personal-data collection; and
f) Follow the separate CCA conformance procedure applicable to production implementations.

7.6. Relying party and document holder

A relying party shall use a current verification solution, review the structured result and evidence freshness, compare verified data with the visible document, conduct any separate identity or entitlement checks and avoid overriding indeterminate or negative results without authority.

The document holder is not responsible for diagnosing cryptographic or infrastructure failures. Issuers shall provide accessible procedures for correction or replacement when verification fails because of erroneous issuance or document lifecycle events.

Annex A - Normative and supporting references

Ref	Document	Use
[1]	ICAO Technical Report - Visible Digital Seal for Non-Constrained Environments (VDS-NC), Release 1.4, 27 May 2022	Technical source basis; Bangladesh does not claim conformity.
[2]	ICAO Doc 9303, Part 12 - Public Key Infrastructure for Machine Readable Travel Documents	Supporting PKI terminology and comparison.
[3]	ICAO Doc 9303, Part 13 - Visible Digital Seals	Supporting VDS terminology and comparison.
[4]	RFC 2119	Normative requirement words.
[5]	RFC 3339	Timestamps.
[6]	RFC 4648	Base64url.
[7]	RFC 5280	X.509 certificates and CRLs.
[8]	RFC 5480	Elliptic-curve SubjectPublicKeyInfo.
[9]	RFC 7493	I-JSON.
[10]	RFC 8392	CBOR Web Token
[11]	RFC 8785	JSON Canonicalization Scheme.
[12]	ISO/IEC 18004, applicable approved edition	QR Code symbology.
[13]	ISO/IEC 15415, applicable approved edition	Two-dimensional barcode print quality.
[14]	The Unicode Standard and Unicode Standard Annex #15	Unicode and NFC normalization.
[15]	Applicable Bangladesh CCA e-seal Certificate Policy and Certification Practice Statement	National certificate issuance, key protection, validity, revocation and rollover.
[16]	PKI Interoperability Guideline of Bangladesh (CCA), applicable approved edition	National profile-authorization registry and PKI interoperability.

Annex B - Abbreviations and key terms

Term	Meaning
CA	Certificate Authority.
CCA	Controller of Certifying Authorities, Bangladesh.
CRL	Certificate Revocation List.
Data Zone	The top-level data object containing hdr and msg and protected by the signature.
Document Issuer Authority	An organization authorized by CCA to sign a registered National Document Profile.
ECDSA	Elliptic Curve Digital Signature Algorithm.
I-JSON	Interoperable JSON profile defined by RFC 7493.
JCS	JSON Canonicalization Scheme defined by RFC 8785.
National Document Profile	A registered bd.<profile> specification for a document family, version and language schema.
Profile-authorisation registry	CCA information mapping a stable organisation identifier and its certificates to permitted bd.<profile> values.
Relying party	A person, organisation or system that relies on a verification result.
Signature Zone	The top-level sig object containing alg, cer and sigvl.
VDS-NC	Visible Digital Seal for Non-Constrained Environments.