IusBubble Webinar #19 (bis 12.45)
und
BAV Digital-Mittag online, 5.3.2025 spezial (bis 13.00)

Validierung von elektronischen Beweismitteln – False Negatives, False Positives und ignorante Validatoren

BAV Digital-Mittag online:

für BAV-Mitglieder und Mitglieder anderer kantonaler Anwaltsverbände

Programm und alle Workshops und Kurse des Bernischen Anwaltsverbands (BAV) zum Thema Digitalisierung:

https://www.bav-aab.ch/de/digitalisierung-justitia-4.0.html

Inhalt

- Validieren, ein Überblick
- Definitionen
- Validierung von elektronischen Beweismitteln – warum?
- Methodik der Validierung in der e-Kanzlei
- Stolpersteine I-XII
- validatoren.ch/prototyp (Prototyp)

Validieren, ein Überblick

Anwendungsbereiche

- Dateien (e-Beweismittel) validieren (bspw. elektronische Signatur)
- Elektronische Archivierung: PDF-Dateien u.a. hinsichtlich Eigenschaften PDF/A-1b validieren, sowie Prüfung JBIG2, andere Dateiformate → weitere Validierungen
- xml-Dateien gegen xml-Schemata validieren
- Akteneinsicht: forensic data validation
- Forensic tools wie Autopsy: validation of forensic methods
- html- und css-Checker für Webseiten
- etc.
- etc.

Definitionen

Verification and validation (v&v) = „a generic term for the complete range of checks that are performed on a system in order to increase confidence that the system is suitable for its intended purpose. [...]
Altough the precise distinction is not always drawn

- the **verification aspect** normally refers to completely objective checking of conformity to some well-defined specification
- while the **validation aspect** normally refers to the somewhat subjective assessment of likely suitability in the intended environment.“ [...]

(Oxford Dictionnary of Computer Science, 2016, p. 587)

validator.admin.ch: „Mit dem Validator können elektronisch signierte Dokumente beziehungsweise in diesen Dokumenten enthaltene elektronische Signaturen auf ihre Gültigkeit geprüft werden.“

Definitionen

validation = process of verifying and confirming that a certificate or a digital signature is valid

signature validation = „process of verifying and confirming that a digital signature is technically valid”

signature verification = “process of checking the cryptographic value of a signature using signature verification data”

Quelle: ETSI EN 319 102-1 V1.3.1 (2021-11): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

Wobei: AdES = Advanced Electronic Signatures

Validierung von elektronischen Beweismitteln – warum?

- Dateien weisen bestimmte **elektronische Eigenschaften** auf, die einen Einfluss auf die Beweiskraft haben können, die diesen Dateien zugewiesen werden: a) Entstehungskontext der Dateien, b) Vollständigkeit der Dateien, c) Veränderungen, etc.
- (Und im Notariat: Dateien weisen bestimmte Eigenschaften auf, die bei der EzuP und der EzuE-Beglaubigung nach EÖBV von Bedeutung sind.)
- Wer elektronische Beweismittel in ein Verfahren einbringen möchte bzw. wer Zweifel an der Beweiskraft elektronischer Beweismittel susbstanziieren will, kommt um das Validieren nicht herum.
- Auch hier: Ein Stück Papier ist nicht dasselbe wie eine Datei. → Validierung von elektronischen Beweismittel unterscheidet sich grundlegend von der Validierung eines in Papierform vorliegenden Beweismittels.

Validierung von elektronischen Beweismitteln – warum?

dass ausserdem zwar die Eingabe der Rechtsvertreterin der Beschwerdeführenden vom 28. Januar 2025 qualifiziert elektronisch signiert hat, aber sämtliche mit dieser Eingabe digital übermittelten Beschwerdeführerbeilagen, die von den angeblichen Ausstellern angeblich digital erstellt worden sind, zwar als Fotokopie (angebliche) digitale Verifizierungsmerkmale enthalten, diese aber informationstechnologisch nicht verifizierbar oder fehlerhaft sind,

https://entscheidsuche.ch/view/CH_BVGE_001_D-7088-2024_2025-02-06

Methodik der Validierung

Checkliste (summarisch)

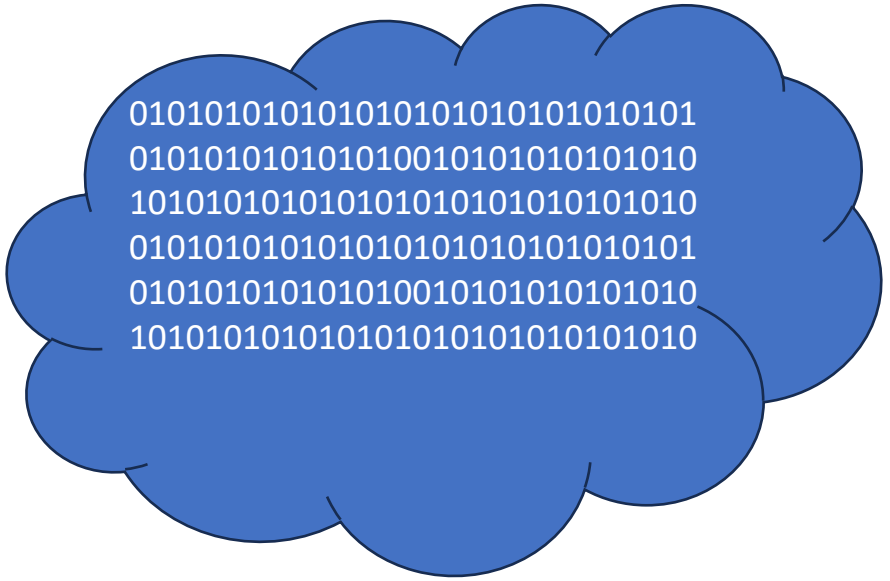
- **Grob-Analyse (forensisch) durchführen:** separate Checklisten, je für Gruppen von Dateiformaten.
- **Erkenntnisinteresse formulieren:** Was will/muss ich über die elektronischen Eigenschaften der vorliegenden Datei wissen?
  - vorhandene elektronische Eigenschaften
  - **nicht** vorhandene elektronische Eigenschaften → Scan Handunterschrift
- **Technische Validierung der Datei:** geeignete Validator**en** auswählen.
- **Rechtliche Interpretation** der Resultate der technischen Validierung der Datei.

Methodik der Validierung

> 1 Validator für eine Datei, wenn diese verschiedene e-Eigenschaften aufweist

PDF/A?

OCR korrekt?



EXIF-Daten vorhanden?

OCR vollständig?

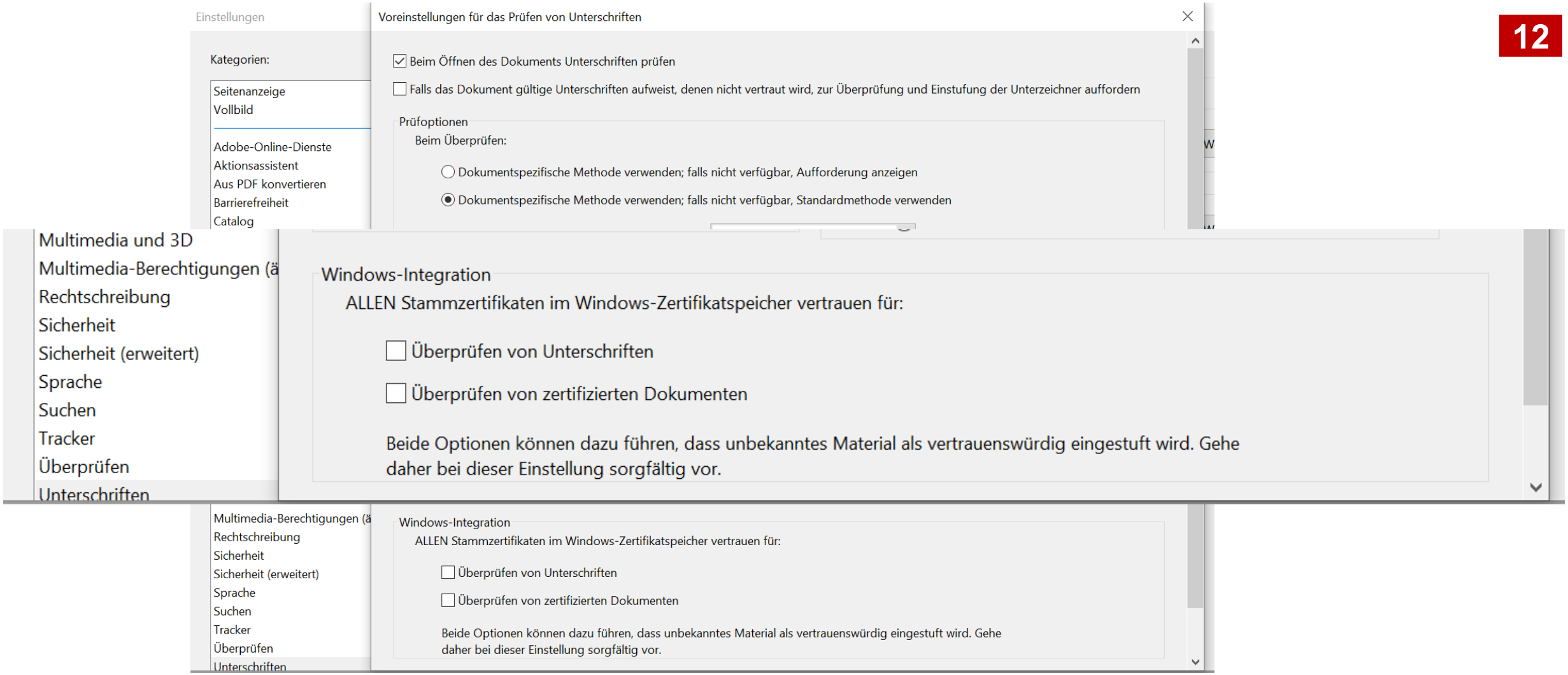
QES valid?
hinsichtlich a, b, c, d, x, y z

Welche Stolperfallen(2) sind hier eingebaut?

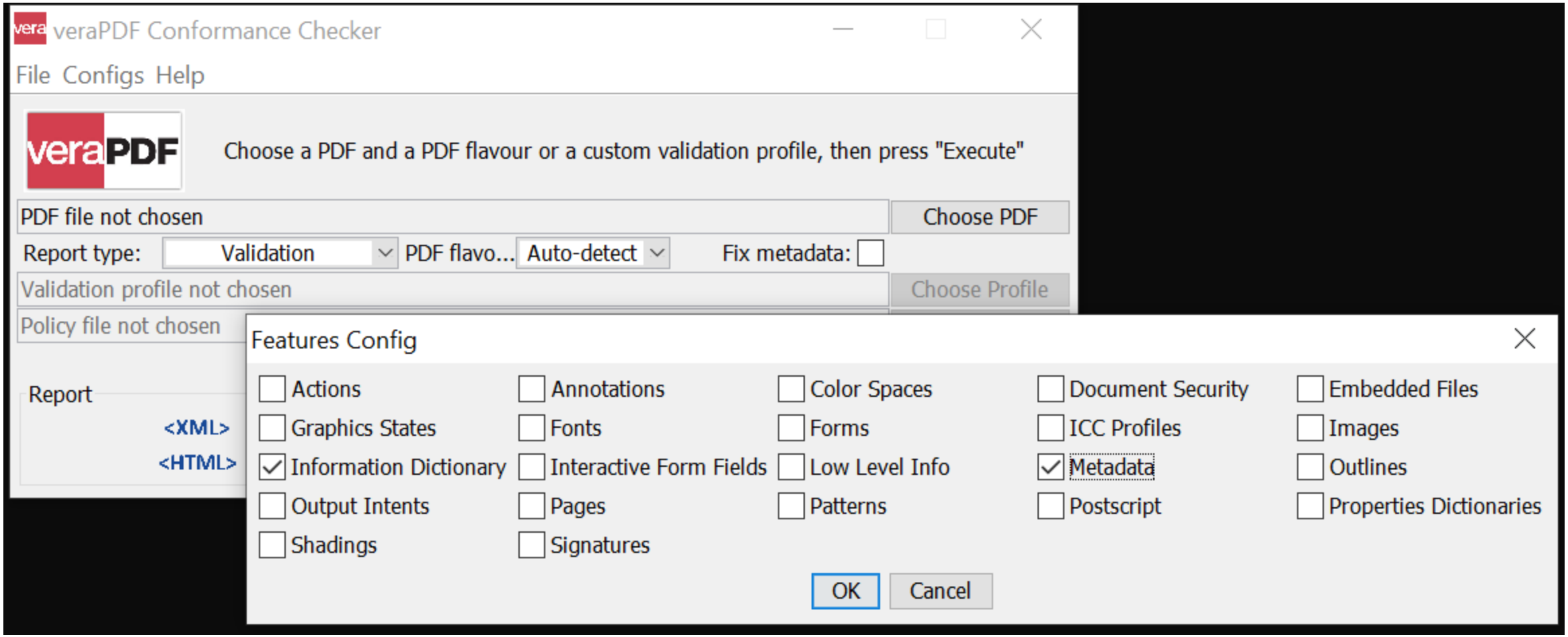
Config-Einstellungen des Validators

- Adobe Acrobat erlaubt es, die Art und Weise, wie elektronische Signaturen geprüft werden, zu konfigurieren. → Resultat einer Validierung ist nur nachvollziehbar, wenn die Einstellungen bekannt sind.
- veraPDF und KOSTVal erlauben es, bestimmte Prüfungen ein- oder auszuschalten
- **Fazit: → auch Konfigurationseinstellungen des Validators, sofern Änderung der Konfiguration durch User möglich, gehören zum Validierungsreport**

Stolpersteine I



Stolpersteine I



Stolpersteine II

Validatoren sind auch nur Softwares...

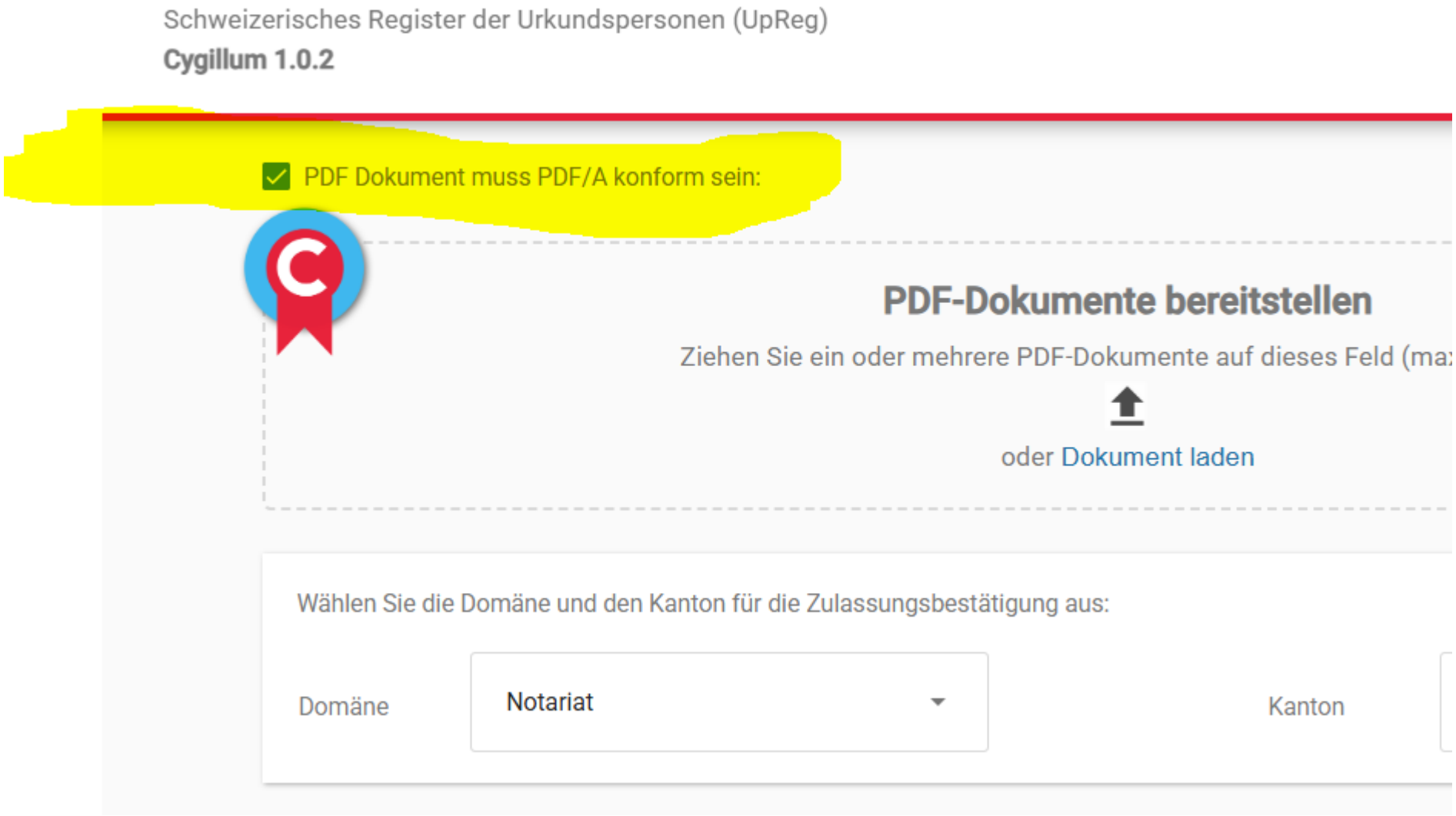
- Eine Version X.1 eines Validators kann zu einem anderen Validierungsergebnis kommen wie die Version X.2 desselben Validators
- Praxisbeispiel: Anmeldung bei Grundbuch in elektronischer Form: Der Notar validiert seine Muster-Dateien mit dem nicht diskreten Webvalidator des Bundes, das Grundbuchamt validiert mit einer älteren Version des diskreten Validator-Clients des Bundes. Ersterer sagt „OK“, letzterer sagt „Nicht OK“
- Quizfrage: Wurde das Geschäft in der Folge vom Grundbuchamt weiter bearbeitet?
- **Fazit: → auch Angaben zur verwendeten Version eines Validators gehören in den Validierungsreport**

Stolpersteine III

Unterschiedliche Interpretationen der Spezifikation

- Eine Datei, drei Validatoren, drei Meinungen
- specification is not „well-defined“
- Praxisbeispiele: PDF/A-1b-Validierung für das e-Notariat und für die elektronische Langzeitarchivierung
- **Fazit: → Workflows müssen die Möglichkeit berücksichtigen, dass der eingesetzte Validator Resultate erzeugt, die nicht über alle Zweifel erhaben sind, ohne dass es sich dabei um false positives bzw. false negatives handelt. Ein Validator darf in solchen Fällen nie ein Show-Stopper sein.**

Stolpersteine III



Stolpersteine IV

False positives

- a test result which wrongly indicates that a particular condition or attribute is present
- Wann liegt ein false positive vor und wann versteht lediglich der User den Validierungsreport falsch?
- Beispiel Viruscheck bei justitia.swiss → Abgabequittung vor Viruscheck
- Beispiel elektronische öffentliche Urkunde nach EÖBV: der Adobe Reader gibt 2x “grünes Licht” für solche Dateien, obwohl dieser Software derzeit die Spezifikation für solche Dateien nicht bekannt sind.
- **Fazit: → Es ist nicht empfehlenswert, den falschen Validator einzusetzen und/oder den Validierungsreport nicht richtig zu interpretieren.** Bei RA/innen und Notar/innen: Sorgfaltspflichtverletzung. Bei Behörden: ...?

Stolpersteine V

False negatives

- test result which wrongly indicates that a condition does not hold

Stolpersteine VI

Ignorante Validatoren (ignorante User?)

- Validator-Software, die sich bspw. zu Eigenschaften von Dateien äussert, die sie effektiv nicht validieren kann, weil eine solche Validierung ausserhalb des Scopes der Validierungssoftware liegt.
- Beispiel PDF-Datei mit einem qualifizierten Zeitstempel
- Beispiel PDF-Datei mit HIN fortgeschrittene elektronische Signatur
- Ad Webvalidator und Validator-Client des Bundes: a) wurden zur Validierung spezifischer Behörden-Dateien entwickelt, b) Scope der Validierung war früher unübergehbar und ist neuerdings wieder halbwegs sichtbar deklariert
- **Fazit: → Der Bundesvalidator ist keine eierlegende Wollmilchsau, auch wenn er sich auf den ersten, oberflächlichen Blick so präsentiert.**

Stolpersteine VI

Hier können elektronisch signierte Dokumente geprüft werden. Falls der Signatur von berechtigter S
angezeigt.

Dokument validieren

Alte Ansicht

1 Wählen Sie den Dokument-Typ

Was für ein elektronisches Dokument möchten Sie auf seine Gültigkeit prüfen?

2

Wählen Sie den Dokumenttyp (Liste)

- Wählen Sie den Dokumenttyp (Liste)
- BAKOM Dokumente
- Validator für Veranlagungsverfügungen und Rückerstattungsbelege der Eidgenössischen Zollverwaltung
- Dokument eines Betreibungsamtes (eSchKG)
- Bundesrecht
- Qualifizierte Signatur mit Zeitstempel gemäss ZertES
- Kanton Zug: Verwaltungsbehörden des Kantons, der Gemeinden oder Verwaltungsgericht
- Qualifizierte Signatur gemäss ZertES
- Strafregisterauszug
- Mit Swiss Government PKI Smartcard und Zertifikat signiertes und zeitgestempeltes Dokument schweizerischer Behörden
- Elektronische öffentliche Urkunden und elektronische Beglaubigungen

3

Organisation:

Dokument validieren

Hier können elektronisch signierte Dokumente geprüft werden. Falls der Signatur von berechtigter Stelle eine amtliche Funktion zugeordnet ist, so wird diese angezeigt.

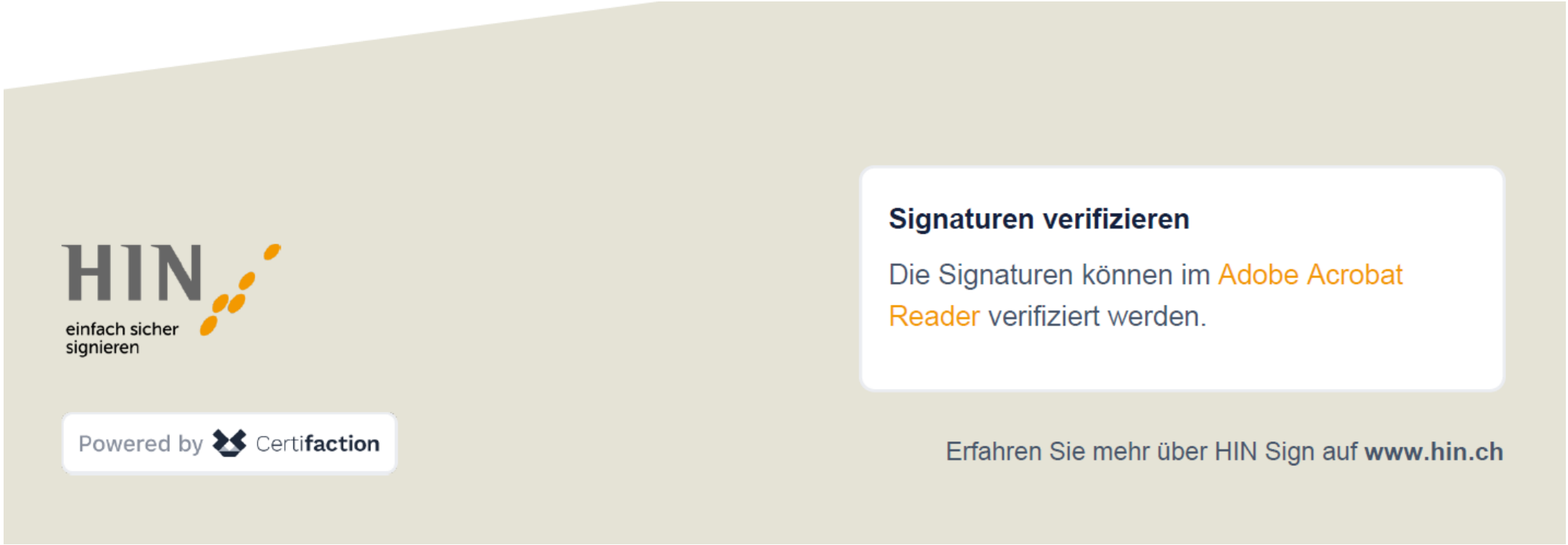
1 Dokument uploaden

Neue Ansicht, Scope nicht auf den ersten Blick ersichtlich

Bitte ziehen Sie Ihr Dokument in dieses Fenster oder klicken Sie hier und wählen Sie eine elektronisch signierte Datei aus, die Sie überprüfen möchten.
Erlaubte Dokumente .pdf / .xml

› Datenschutzerklärung, Informationsschutz und Wahrung von Berufs- oder Amtsgeheimnissen
Erklärung zum Datenschutz

Stolpersteine VI

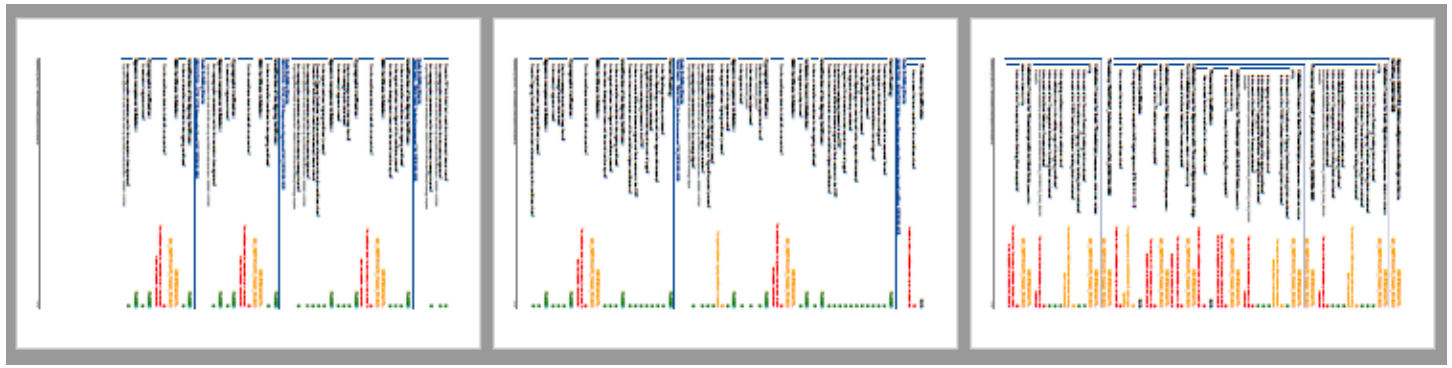


[...] „das ist leider ein altbekanntes Problem mit dem Validator des Bundes. Bei fortgeschrittenen Signaturen liefert dieser leider sehr unglückliche Resultate weshalb wir bei unserer Lösung auch immer auf den Adobe Acrobat Reader verweisen mit dem grünen Häckchen oben links.“

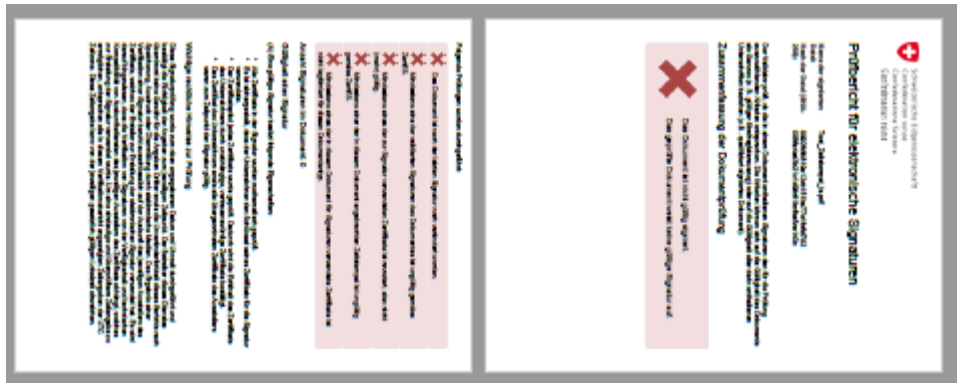
Unklare Resultat-Präsentation im Validierungsreport

- Gemäss ETSI EN 319 102-1 V1.3.1 (2021-11) soll ein Validator, der AdES Digital Signatures validiert, folgende Status-Meldungen pro ”Validierungsblock” abgeben:
  - TOTAL-PASSED
  - TOTAL-FAILED
  - INDETERMINATE
- Vergleich Output Bundesvalidator vs. Output DSS-Testvalidator für Datei mit qualifiziertem elektronischem Zeitstempel
- Notabene: Die beiden Bundesvalidatoren wurden entwickelt, als es den ETSI EN 319 102-1 V1.3.1 (2021-11) noch nicht gab.

Stolpersteine VII



Generated by DSS v.6.1 with validation time 2025-01-14T07:56:19Z1



Webvalidator des Bundes, soweit ersichtlich keine Info zur Version

Stolpersteine VII

Basic Building Blocks
TIMESTAMP - TIMESTAMP_Swiss-Government-TSA_20250108-1633

Identification of the Signing Certificate : PASSED

- Is there an identified candidate for the signing certificate? ✓
- Is the signed attribute: 'cert-digest' of the certificate present? ✓
- Are the issuer distinguished name and the serial number equal? ✓

X509 Certificate Validation : INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

- Can the certificate chain be built till a trust anchor? ✗

The certificate chain for time-stamp is not trusted, it does not contain a trust anchor.

Cryptographic Verification : PASSED

- Has the message imprint data been found? ✓
- Is the message imprint data intact? ✓
- Is time-stamp's signature intact? ✓

Stolpersteine VII

Folgende Prüfungen wurden durchgeführt:

- ✗ Das Dokument ist nach der letzten Signatur noch verändert worden.
- ✗ Mindestens eine der validierten Signaturen des Dokumentes ist ungültig gemäss ZertES.
- ✗ Mindestens eines der zur Signatur verwendeten Zertifikate ist revoziert, also nicht (mehr) gültig.
- ✗ Mindestens einer der in diesem Dokument angebrachten Zeitstempel ist ungültig gemäss ZertES.
- ✗ Mindestens eines der in diesem Dokument für Signaturen verwendete Zertifikate ist nicht legitimiert für diesen Dokumententyp.

Anzahl Signaturen im Dokument: 0

Interpretation eines Validierungsreports

- Auch wenn der Validierungsreport aus der Validierung einer elektronischen Eigenschaft einer Datei, die im Scope der Validatorsoftware liegt, entstanden ist, ist die Interpretation nicht banal. Insbesondere bei älteren Dateien...
- Es stellen sich zahlreiche Fragen, bspw.
  - Muss das Zertifikat einer QES noch gültig sein, wenn es darum geht, zu beweisen, dass eine Datei oder ein Teil einer Datei seit Anbringen einer e-Signatur nicht verändert wurde?
  - Muss ein QES-Zertifikat mit einem qualifizierten Zeitstempel zusammen verwendet worden sein, um zu beweisen, dass eine bestimmte Dabei an einem bestimmten Zeitpunkte existierte?
- Wenn ein RA ein e-Beweismittel einreicht, soll er/sie auch einen kommentierten Validierungsreport einreichen, um Missverständnisse zu vermeiden?

Stolpersteine IX ff.

- Validator nicht öffentlich verfügbar
- Validator nicht diskret öffentlich verfügbar
- Validierungsreport nicht verkehrsfähig

Prototyp https://validatoren.ch/prototyp/

Versuch:

- Sensibilisieren
- Übersicht erstellen

Mitstreiter/innen gesucht:

- Soll das Vorhaben fortgesetzt werden?
- Trägerschaft? (bisher: Fachgruppe Validatoren der Digitalen Gesellschaft, Inhalte: Claudia Schreiber)

Prototyp validatoren.ch/prototyp

Prototyp der Validatorenliste

Legende: DI = nicht-diskrete Validierung; DI = diskrete(re) Validierung; VR = es wird ein verkehrsfähiger Validierungsreport erstellt; VR = es wird kein verkehrsfähiger Validierungsreport erstellt; ÖF = der Validator ist unentgeltlich öffentlich zugänglich; ÖF = der Validator ist nicht oder nicht unentgeltlich öffenlich zugänglich;

To do: Credits, Schriften/Ressourcen lokal einbinden

Show 10 entries

Search:

Land	Bereich	Zu validierende elektronische Eigenschaft	Dateiformate	gesetzliche Grundlage	Validator/Software	Eigenschaften	Validator wird zur Verfügung gestellt durch	Desiderata	Status Eintrag	Letzte Prüfur
CH	Recht, amtliche Dateien	eDec: Dateien des Bundesamtes für Zoll und Grenzsicherheit (BAZG)	PDF	Zollgesetz ZG, SR 631.0	Online-Service	DI VR	Bundesverwaltung, Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei	a) Info zu release version, b) diskreter Webvalidator	OK	10.23
CH	Recht, amtliche Dateien	SG-PKI: Datei enthält gültige Swiss Government PKI Signature(n) mit Zeitstempel	PDF							
CH	Recht, amtliche Dateien	Amtsblatt-Portal: Dateien als offizielle amtliche Meldungen	PDF							
CH	QES	der eigenhändigen Unterschrift gleichgestellte QES mit qualifiziertem Zeitstempel	PDF	ZertES und OR Art. 14 Abs. 2bis	Online-Service	DI VR	Bundesverwaltung, Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei	a) Info zu release version, b) diskreter Webvalidator	OK	10.22
CH	QES	der eigenhändigen Unterschrift gleichgestellte QES mit qualifiziertem Zeitstempel	PDF	ZertES und OR Art. 14 Abs. 2bis	API, diskreter eGov-Validator	DI VR ÖF	Bundesverwaltung, Bereich Digitale Transformation und IKT-Lenkung		OK	10.23

Fragen, Diskussion