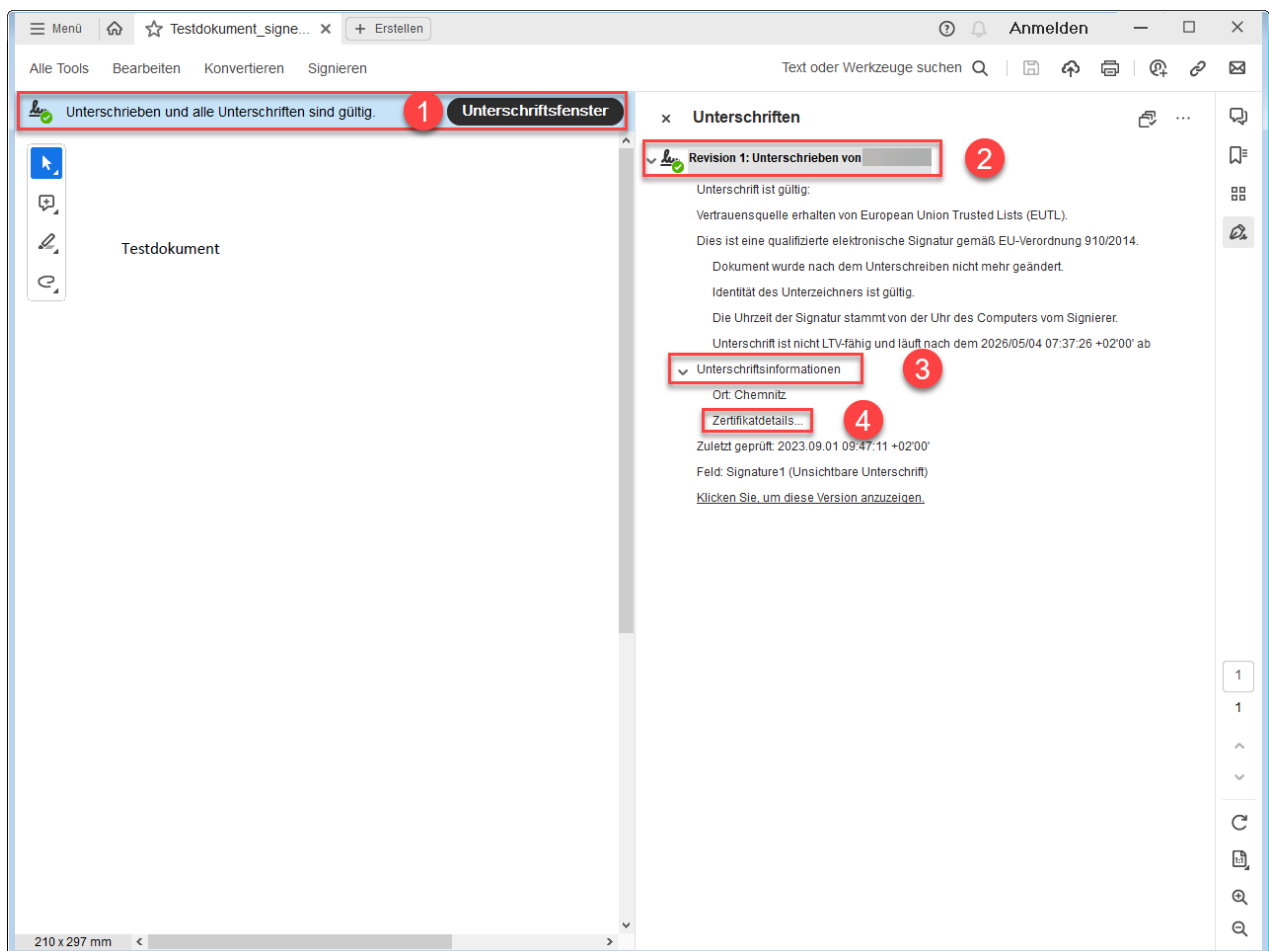


1 Vorbemerkung

Die Validierung einer qualifizierten E-Signatur (QES) eines PDF-Dokuments erfolgt im Anzeigeprogramm derjenigen Person, die das elektronisch signierte Dokument aufruft. Für die Validierung ist keine Signaturkarte erforderlich.

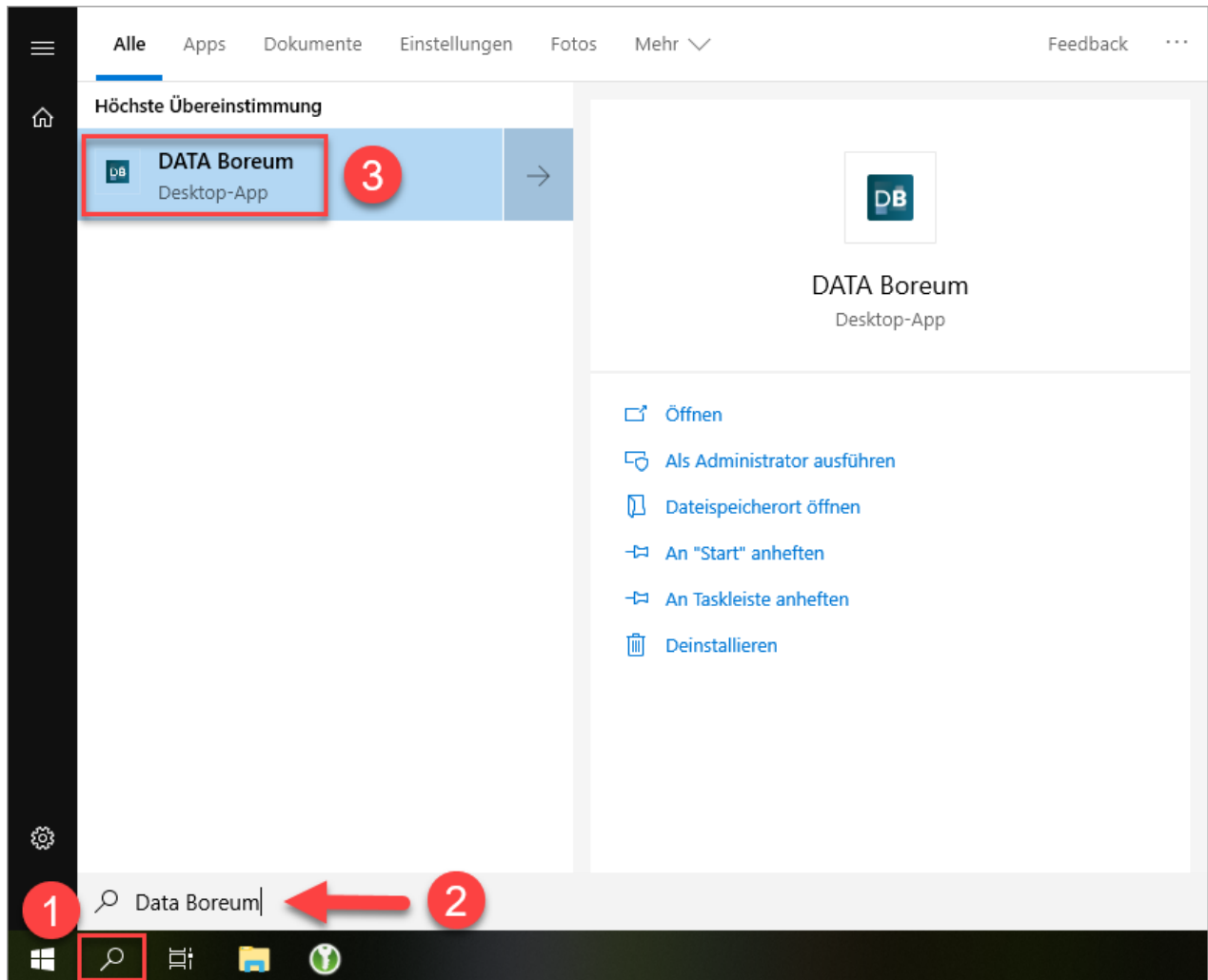
2 Validierung in Adobe Acrobat Reader

Öffnen Sie das zu überprüfende PDF-Dokument in **Adobe Acrobat**. Ihnen wird nun in der Kopfzeile des Dokuments automatisch ein **Banner** angezeigt, ob Signaturen enthalten und diese gültig sind. Falls Sie weitere Informationen abrufen möchten, dann klicken Sie auf **Unterschriftsfenster**. Im sich öffnenden Bereich **Unterschriften** wählen Sie die Signatur aus, die Sie überprüfen möchten und klappen diese über den kleinen Pfeil auf. Bei einer QES sollte Ihnen angezeigt werden, dass es sich um **eine qualifizierte elektronische Signatur gemäß EU-Verordnung 910/2014** handelt. Um sich Details zum Aussteller der Signatur oder zum Vertrauensdienstanbieter anzeigen zu lassen, klappen Sie **Unterschriftsinformationen** auf und klicken Sie auf **Zertifikatsdetails**.

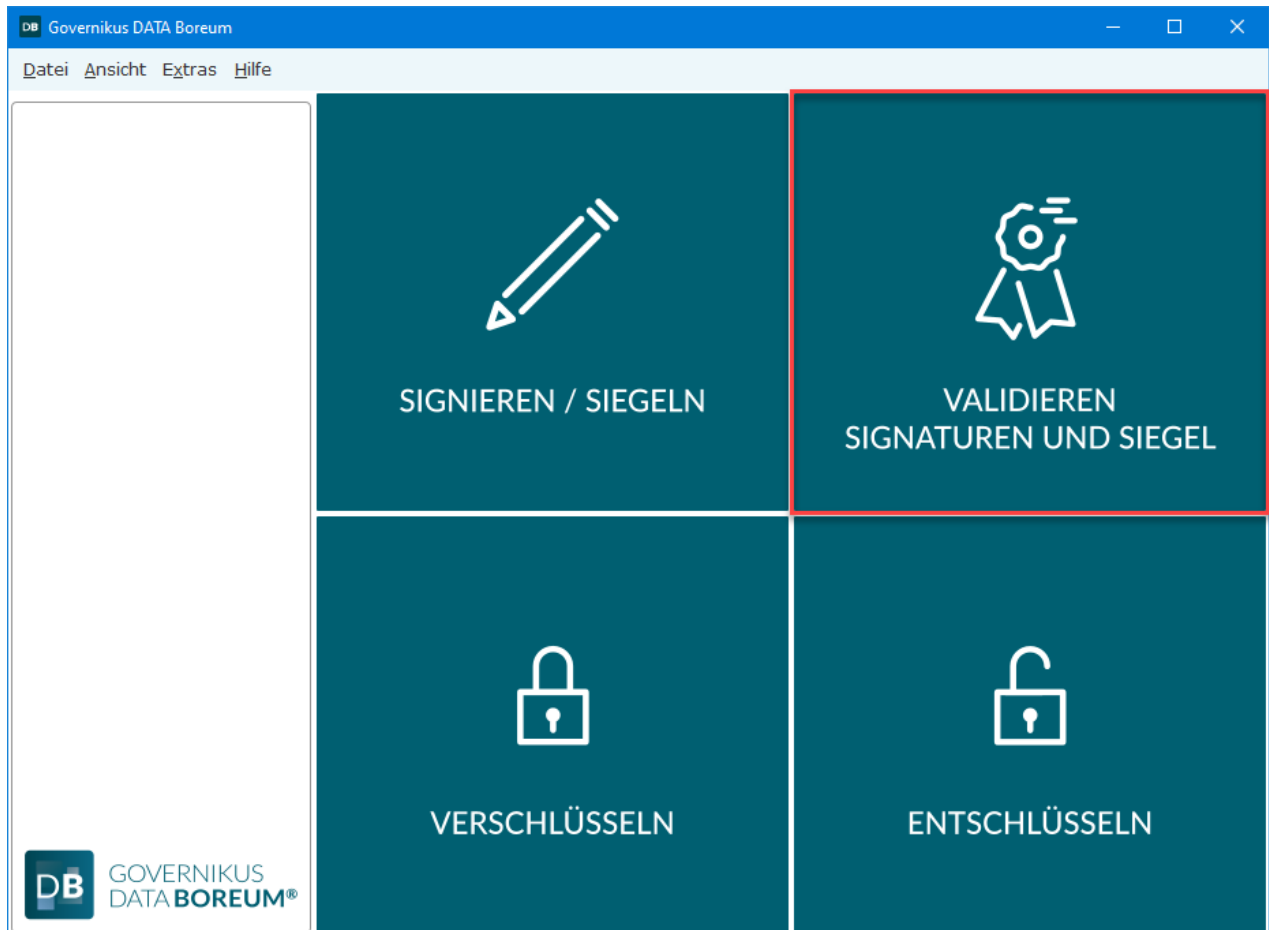


3 Validierung in DATA Boreum

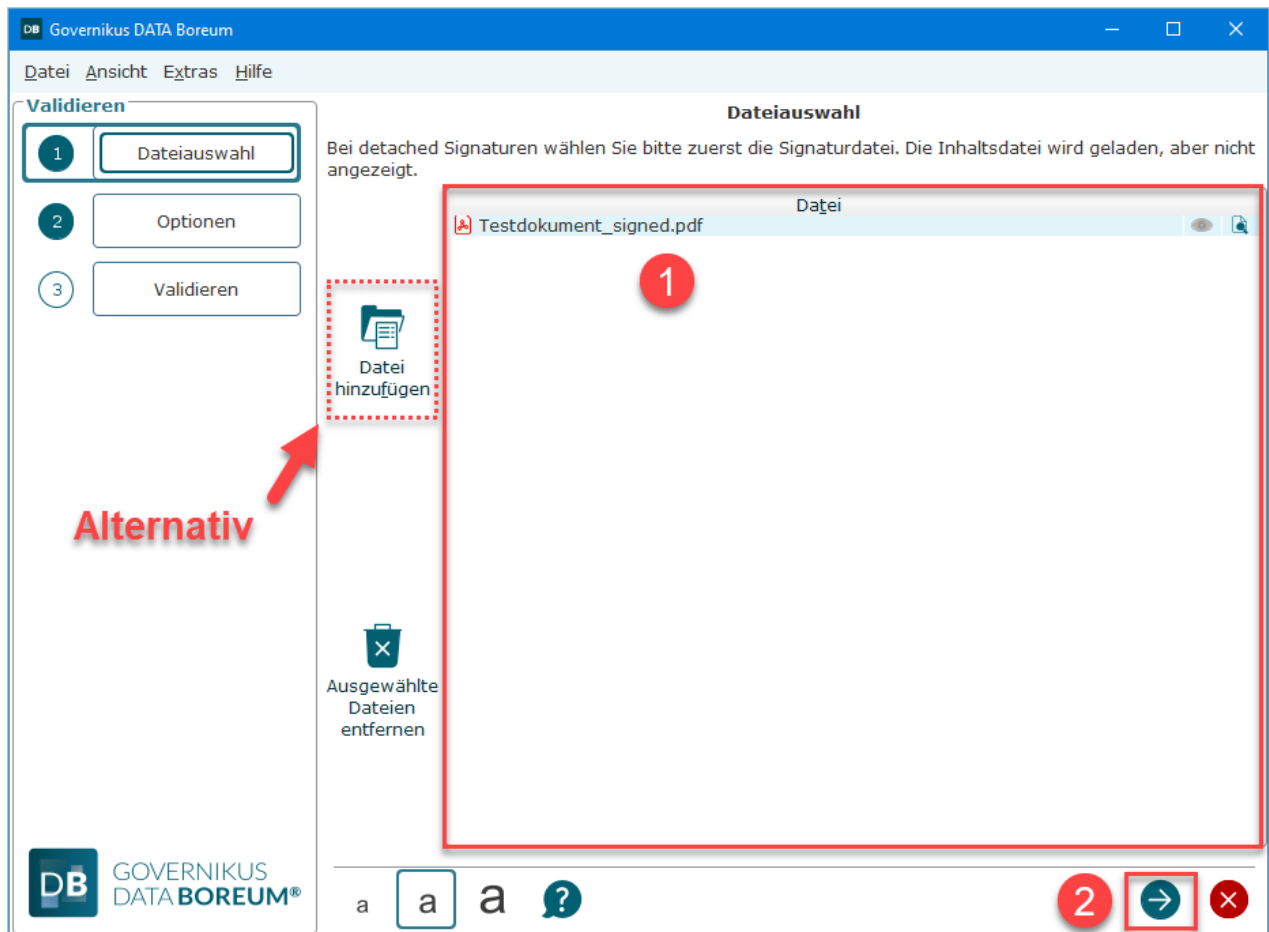
Öffnen Sie die Desktop-App **DATA Boreum**. Diese können Sie im Windows-Startmenü aufrufen, indem Sie in der Taskleiste auf das Suchsymbol klicken und nach dem Namen der App suchen.



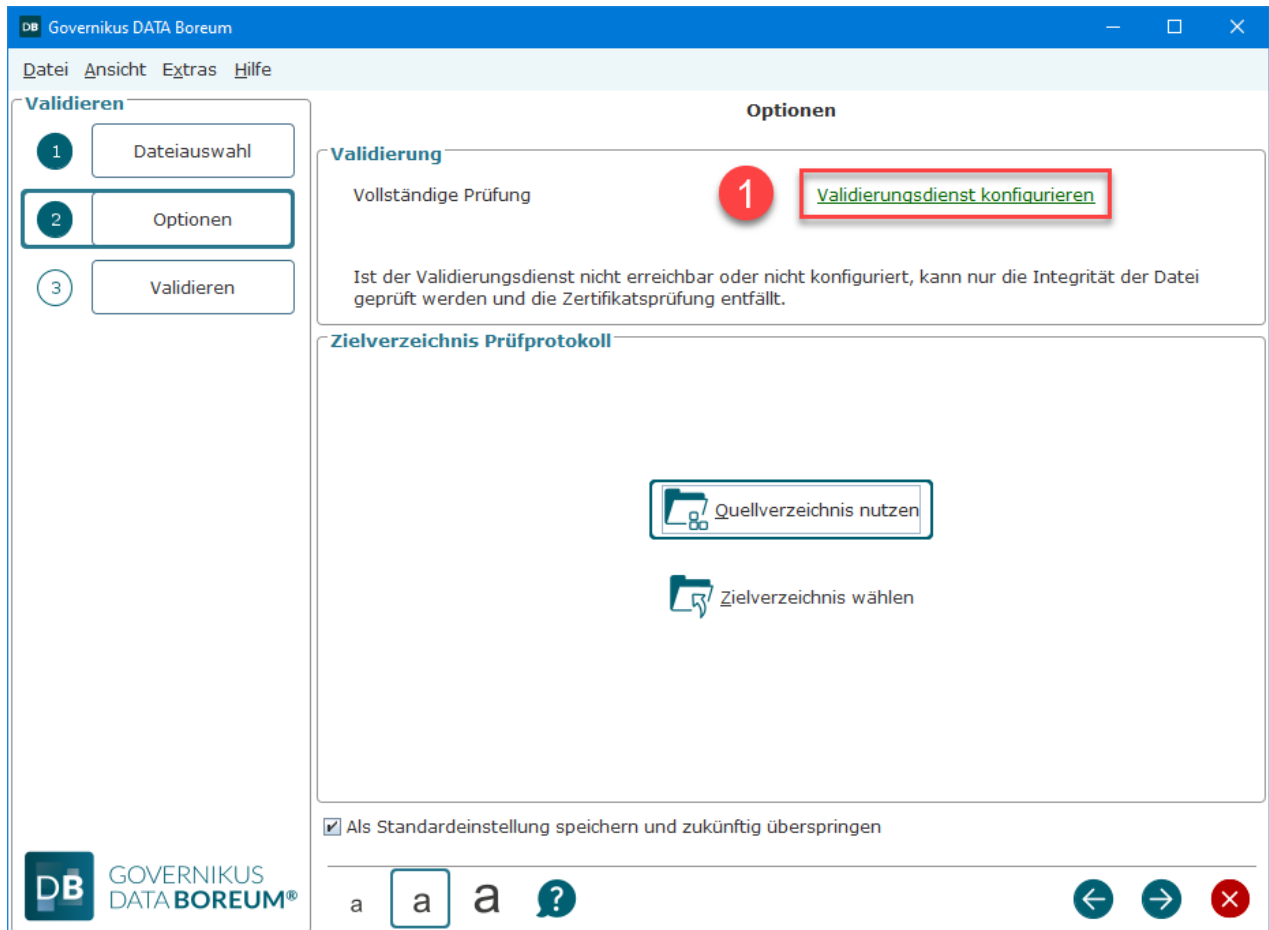
Wählen Sie **Validieren - Signaturen und Siegel**.



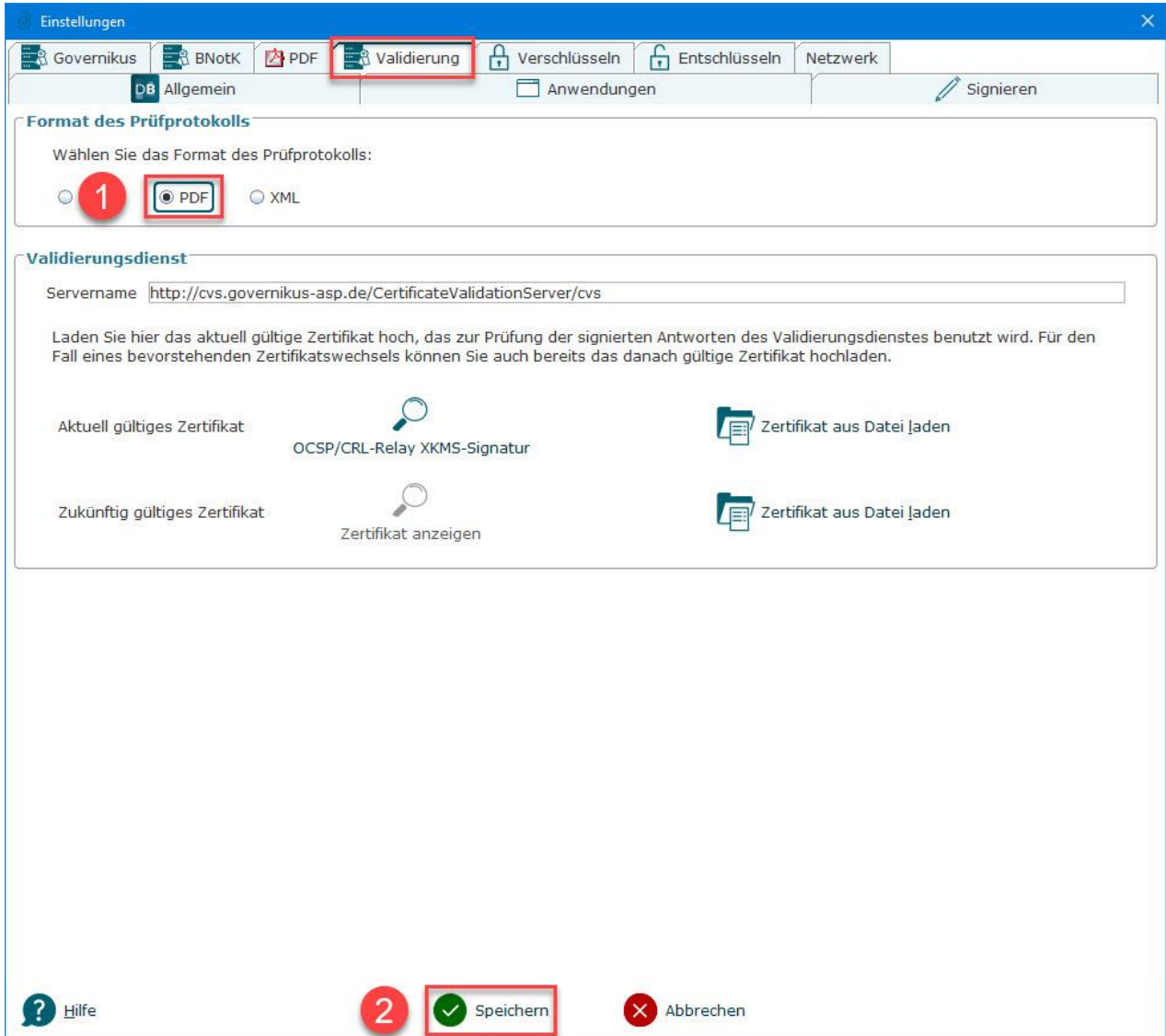
Sie befinden sich nun im **Schritt 1 Dateiauswahl**. Ziehen Sie mit der Maus das zu überprüfende Dokument in den leeren Bereich unter **Datei**. Alternativ können Sie über das Feld **Datei hinzufügen** ein Dokument auswählen. Klicken Sie auf den **Vorwärtspfeil**, um zum nächsten Schritt zu gelangen.



Im **Schritt 2 Optionen** klicken Sie auf **Validierungsdienst konfigurieren**.



Im darauf erscheinenden Fenster wählen Sie im Reiter **Validierung** unter **Format des Prüfprotokolls** die Option **PDF** aus. **Speichern** Sie die Änderung.



Einstellungen

Governikus BNotK PDF **Validierung** Verschlüsseln Entschlüsseln Netzwerk

DB Allgemein Anwendungen Signieren

Format des Prüfprotokolls



Wählen Sie das Format des Prüfprotokolls:



☐ 1 ☒ PDF ☐ XML

Validierungsdienst

Servername

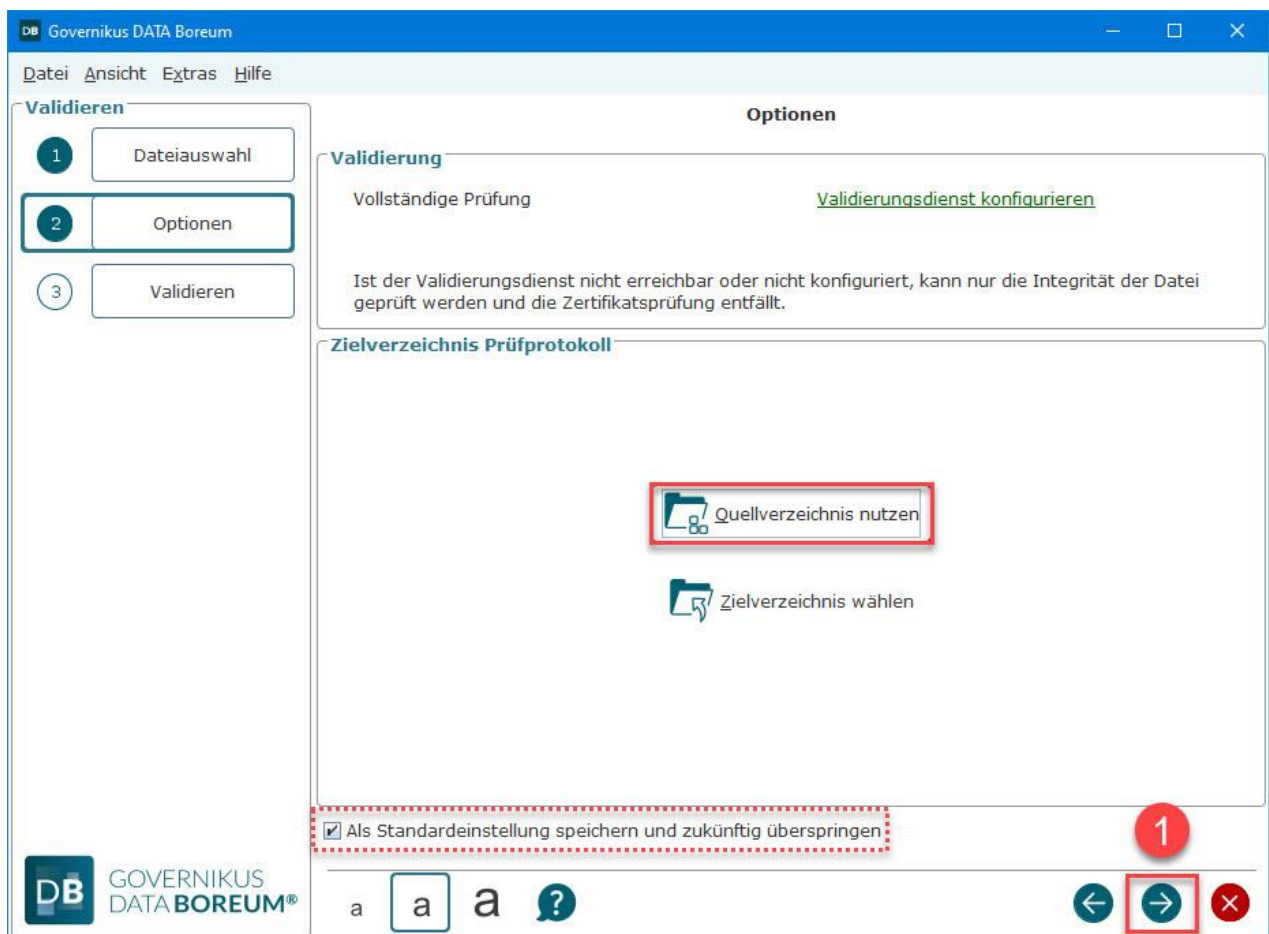
Laden Sie hier das aktuell gültige Zertifikat hoch, das zur Prüfung der signierten Antworten des Validierungsdienstes benutzt wird. Für den Fall eines bevorstehenden Zertifikatswechsels können Sie auch bereits das danach gültige Zertifikat hochladen.

Aktuell gültiges Zertifikat   Zertifikat aus Datei laden

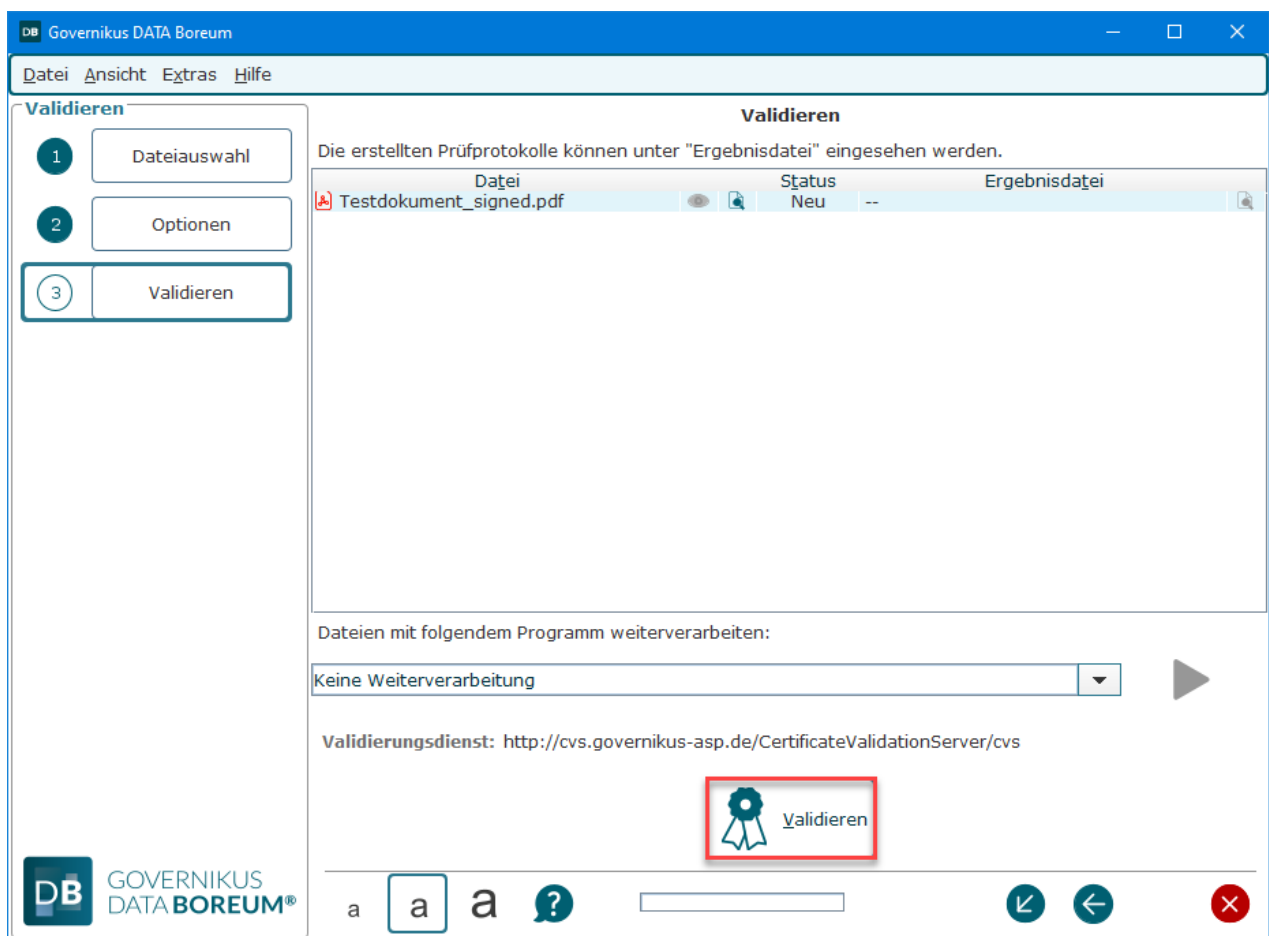
Zukünftig gültiges Zertifikat   Zertifikat aus Datei laden

Hilfe 2

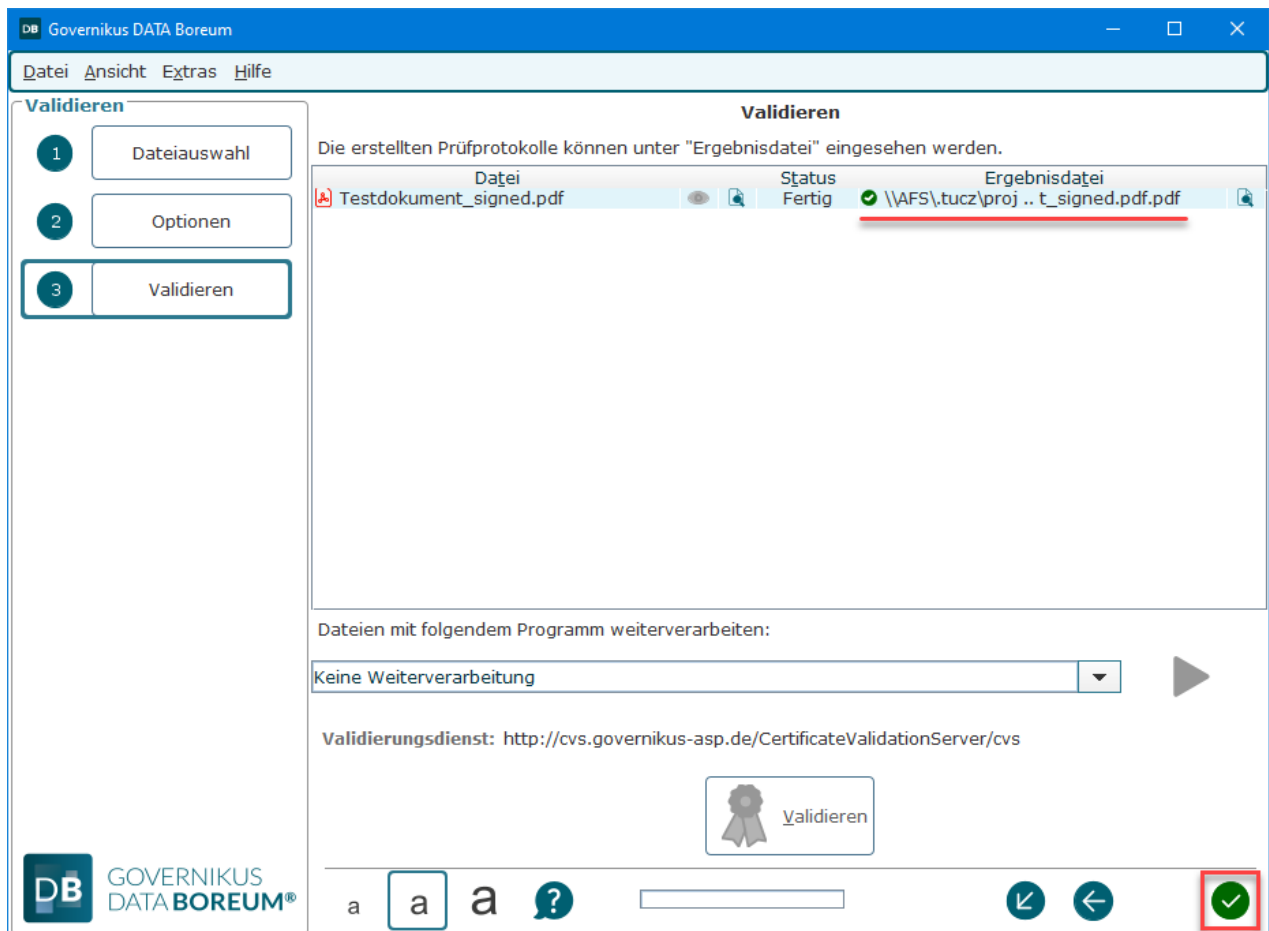
Im **Schritt 2 Optionen** kann die standardmäßig eingestellte Option **Quellverzeichnis nutzen** beibehalten werden. Es wird empfohlen, den Haken auch bei **Als Standardeinstellung speichern und zukünftig überspringen** zu setzen. Bei einem erneuten Aufrufen von DATA Boreum wird daraufhin die aktuelle Ansicht übersprungen. Dies bietet sich an, da die Einstellungen für die Validierung einer qeSignatur in der Regel unverändert bleiben. Klicken Sie auf den **Vorwärtspfeil**, um zum nächsten Schritt zu gelangen.



Im **Schritt 3 Validieren** klicken Sie auf **Validieren**. An dieser Stelle wird das in dem Dokument enthaltene Zertifikat über den Validierungsdienst von Governikus an den herausgebenden qualifizierten Vertrauensdiensteanbieter geschickt, weshalb eine **bestehende Internetverbindung** benötigt wird. Der Vertrauensdiensteanbieter überprüft das Zertifikat auf Echtheit und Gültigkeit. Das signierte Dokument selbst verbleibt hingegen auf dem Rechner und wird lokal auf Integrität geprüft. Warten Sie auf die Meldung, dass der Validierungsvorgang erfolgreich abgeschlossen wurde.



Nach der Validierung wird im Zielverzeichnis ein **Prüfprotokoll** erzeugt, das zusätzlich zum ursprünglichen Dateinamen des Originaldokuments die Ergänzung **pdf.pdf** trägt (in dieser Anleitung heißt das Prüfprotokoll entsprechend Testdokument_signed.pdf.pdf). Am **ausgegrauten Feld Validieren** ist zu erkennen, dass der Signiervorgang abgeschlossen ist. Das Fenster kann nun mit einem Klick auf den Haken geschlossen werden.



Öffnen Sie das erstellte **Prüfprotokoll**, um zu sehen, ob die Validierung erfolgreich verlaufen ist.

Seite 1 von 15

Prüfprotokoll: 31.08.2023, 16:32:27 MESZ

Fachliche Prüfung:

Fachliche Prüfrichtlinie: Ergebnis der fachlichen Prüfung: Meldungen:	Kumuliertes Ergebnis der einzelnen Signaturprüfungen ohne Berücksichtigung des Signaturniveaus. <div style="background-color: green; color: white; text-align: center; padding: 2px;">gültig</div> Alle geprüften elektronischen Signaturen sind gültig.
---	--

Zusammenfassung Dokumente und Signaturprüfungen:

Nr.	Dokument	Signiert durch	Signaturniveau	Signaturprüfung
1.	Testdokument_signed_Revision2.pdf		EU-qualifizierte elektronische Signatur (EUMS-TL)	<div style="background-color: green; color: white; text-align: center; padding: 2px;">gültig</div>

Dokument bzw. Containerstruktur:

PDF-Dokument: Testdokument_signed.pdf

2. Revision

Signatur durch:

Ergebnis der Signaturprüfung:

gültig

Hinweis: Das gesamte Dokument wurde elektronisch signiert.

1. Revision

PAdES: Testdokument_signed_Revision2.pdf

Zeitpunkt der Durchführung der Prüfung:	31.08.2023, 16:32:27 MESZ
Signierte Datei oder Inhalt:	Testdokument_signed_Revision2.pdf
Signatur durch:	
Adresse:	Chemnitz
Niveau und Typ der Signatur:	EU-qualifizierte elektronische Signatur (EUMS-TL)
Behaupteter Signaturzeitpunkt:	31.08.2023, 15:28:59 MESZ
Prüfzeitpunkt der Signatur:	Behaupteter Signaturzeitpunkt
Ergebnis der Signaturprüfung:	<div style="background-color: green; color: white; text-align: center; padding: 2px;">gültig</div>

PAdES-Signatur B: Testdokument_signed_Revision2.pdf

Zeitpunkt der Durchführung der Prüfung:	31.08.2023, 16:32:27 MESZ
Signierte Datei oder Inhalt:	Testdokument_signed_Revision2.pdf
Signatur durch:	