Release Notes

Governikus DATA Boreum

Governikus DATA Boreum, Release 10.10.1

Inhaltsverzeichnis

Rechtliche Informationen und weitere Hinweise

Obwohl diese Produktdokumentation nach bestem Wissen und mit größter Sorgfalt erstellt wurde, können Fehler und Ungenauigkeiten nicht vollständig ausgeschlossen werden. Eine juristische Verantwortung oder Haftung für eventuell verbliebene fehlerhafte Angaben und deren Folgen wird nicht übernommen. Die in dieser Produktdokumentation enthaltenen Angaben spiegeln den aktuellen Entwicklungsstand wider und können ohne Ankündigung geändert werden. Künftige Auflagen können zusätzliche Informationen enthalten. Technische und orthografische Fehler werden in künftigen Auflagen korrigiert.

1 Version 10.10.1

Veröffentlichung: 05.02.2025

Online-Update über den Installer

Ein Online-Update der Version 10.10.0 auf Version 10.10.1 ist **möglich**.

Verbesserungen und Fehlerbehebungen

- **Suffix beim Erstellten Prüfprotokoll:** Der Dateiname vom Validierungsprotokoll kann auf Wunsch um „_validation-protocol“ ergänzt werden, um eine bessere Unterscheidung zu signierten Dokumenten treffen zu können.
- **Testzertifikate im Toolkit erneuert:** Die Testzertifikate bzw. Testschlüssel, die dem Toolkit beiliegen, wurden erneuert und sind gültig bis zum 31.12.2029
- **Temporäre Dateien löschen:** Es wurde ein Fehler im Umgang mit nicht gelöschten temporären Dateien, die im Signierprozess angelegt wurde.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.12.5:**
  - Die Kartenerkennung der D-Trust Card 5.x wurde erweitert. Es werden auch die Karten mit dem Zusatz „2cc“ unterstützt, die ab 01/2025 vom Hersteller ausgegeben werden.
- **Kleinere Fehlerbehebungen und Optimierungen**

2 Version 10.10.0

Veröffentlichung: 27.11.2024

Online-Update über den Installer

Ein Online-Update der Version 10.9.3 auf Version 10.10.0 ist **möglich**.

Verbesserungen und Fehlerbehebungen

- **Einstellung für sichtbares Signaturfeld**: Wird ein sichtbares Signaturfeld für PDF-Dokumente eingestellt, können nun die Beschriftungen für z.B. Ort oder den Grund ein- oder ausgeblendet werden, als auch in ihrer Reihenfolge geändert werden.
- **Ver- und Entschlüsselung** auf Basis von Signaturkarten wurde entfernt.
- **Fehlerbehebung bei Signaturabbruch:** Wurde der Signaturprozess in DATA Boreum IE/WE mit einer Signaturkarte abgebrochen, kam es in seltenen Fällen zu einer falschen positiven Meldung („Der Signaturprozess wurde erfolgreich abgeschlossen“) und Boreum wurde nicht geschlossen. Der Fehler wurde behoben und an die aufrufende Fachanwendung wird der Fehlercode `TOO_MANY_WRONG_PINS` zurückgemeldet.
- **Merken der PIN:** Mit dem Parameter `<usePinCache>` ist es möglich, die PIN in DATA Boreum IE/WE temporär zu speichern.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.
- Einbindung der aktuellen Kartenansteuerung (MCard) 2.12.4:
  - Es wird eine neue Terminalserver-Kombination bestehend aus

    Windows Server 2022, Citrix Virtual Apps and Desktops 7 2402 LTSR und

    Windows 11 Client unterstützt
  - Mit dieser Version ist der Einsatz von macOS Sequoia freigegeben.
- **Einbindung einer aktuellen CLS:** Das Release der Version **3.6.4** umfasst im Bereich Validate folgende Änderungen im Vergleich zur Vorversion:
  - Fix für PDF-Signaturen der Bundesagentur für Arbeit.
  - Fix eines Fehlers bei der Erstellung des PDF-Prüfprotokolls.

    Trat nur bei berufsbezogenen Attributen in Zertifikaten auf.

An- und Abkündigungen

Mit der DATA Boreum Version 10.10.0 werden Signaturkarten für die Funktionen Ver- und Entschlüsselung nicht mehr unterstützt.

3 Version 10.9.3

Veröffentlichung: 12.09.2024

Online-Update über den Installer

Ein Online-Update der Version 10.9.0 auf Version 10.9.3 ist **möglich**.

Verbesserungen und Fehlerbehebungen

- **Hotfix:** Mit diesem Hotfix wird die Unterstützung der Karte „Medisign HBA“ unterstützt.

4 Version 10.9.2

Veröffentlichung: 12.08.2024

Online-Update über den Installer

Ein Online-Update der Version 10.9.0 auf Version 10.9.2 ist **möglich**.

Verbesserungen und Fehlerbehebungen

- **Hotfix:** Bei der Eingabe von Zugangsdaten bei der Authentifizierung gegenüber DATA Deneb kam es unter Umständen zu Problemen. Die Zugangsdaten wurden erst nach mehrmaliger Eingabe verwendet.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

5 Version 10.9.1

Veröffentlichung: 17.07.2024

Online-Update über den Installer

- Ein Online-Update der Version 10.9.0 auf Version 10.9.1 ist **möglich**.
- Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.2.3) zu verwenden.
- Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 17.

Verbesserungen und Fehlerbehebungen

- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.
- **Sichtbare Signaturen mit Signaturvorlage:** Es wurde ein Fehler beim Laden der Standardgrafik behoben, die bei der Signaturvorlage verwendet werden kann.
- **Validierungsdienst:** Der Validierungsdienst wird nun in der Standardkonfiguration mit HTTPS anstatt HTTP ausgeliefert.
- **Bessere Fehlerdarstellung bei PAdES-Signaturen:** Kommt es zu einem Fehler bei der Anbringung einer PAdES-Signatur, lassen sich Details dazu anzeigen, um den Fehler besser einzugrenzen
- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.5.2):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:
  - Angepasste Niveaubestimmung (Anpassung an die Aktualisierung der 119 172-14 und 119 615)
  - Änderungen der Niveaubestimmung von Zertifikaten
  - QSCD Bestimmung
  - Notwendige Änderungen an Validierung von QES durch Änderung der Niveaubestimmung
  - QTST nach neuen ETSI-Standard
  - Anpassung Validierung im fortgeschrittenen Bereich (Anlehnung an qualifizierten. Bereich)
- **Speicherkonfiguration:** Unter Umständen kann es passieren, dass DATA Boreum aufgrund der JVM einem höheren Arbeitsspeicherverbrauch unterliegt. Der Konfigurationsparameter `-XX:+UseZGC` hilft dabei, den Verbrauch zu steuern. Dieser ist im Anwendungshandbuch im Kapitel 11.11 dokumentiert.

6 Version 10.9.0

Veröffentlichung: 10.04.2024

Online-Update über den Installer

- Ein Online-Update der Version 10.8.2 auf Version 10.9.0 ist **möglich**.
- Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.2.2) zu verwenden.
- Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 17.

Verbesserungen und Fehlerbehebungen

- **Einbindung der aktuellen Kartenansteuerung (MCard**) **2.12.1:** Mit dieser Version werden die Karten des Anbieters D-Trust in der Version 5.1 Multi und 5.4 Multi unterstützt.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.
- **Fehler beim Signieren mit einem defekten Schlüssel**: Wird ein korruptes Schlüsselmaterial beim Signieren ausgewählt, so wird eine Fehlermeldung ausgegeben und Boreum stürzt nicht mehr ab.
- **Portable-Version Anwenderfreundlicher gestaltet:**
  - Mit einem Parameter kann nun gesteuert werden, ob die Konsole im Hintergrund ein- oder ausgeblendet wird (im Standard ausgeblendet)
  - Die Startverknüpfung hat nun das Boreum-Icon
- **Kein Abbruch im Signiervorgang:** Werden mehrere Dateien zum Signieren (PAdES) zu Boreum hinzugefügt, kann nun ausgewählt werden was passieren soll, wenn eine Datei nicht bearbeitet werden kann, anstatt den gesamten Vorgang abzubrechen.
- **Fehler in der Signaturfeldanbringung behoben:** Es wurde ein Anzeigeproblem im Editor zum Anbringen von sichtbaren Signaturen behoben.
- **Separate Anzeige von fehlerhaften Dateien:** Werden fehlerhafte Dateien (leere PDF-Dateien, passwortgeschützte Dateien, nicht vorhandene Dateien) zu Boreum hinzugefügt, können die Fehlermeldungen nun zusätzlich zum Mouseover via einen Klicks auf das entsprechende Warnsymbol angezeigt werden.
- **Auswertung von PAC-Dateien**: Nutzung einer neuen Bibliothek zur Auswertung von PAC-Dateien. Die bisher verwendete Bibliothek ist ab Java 15 aus JRE entfernt und in diese MSI-Version wird durch die neue Bibliothek ersetzt.

An- und Abkündigungen

- Mit der DATA Boreum Version 10.10.0 werden Signaturkarten für die Funktionen Ver- und Entschlüsselung nicht mehr unterstützt.
- Abkündigung der Supportunterstützung von Java 11 in der Offline-Variante:
  - Die Anwendung ist lauffähig unter Java 11 und Java 17. Der Oracle-Support für Java 11 endete im September 2023.
  - Der Support von Java 11 wird daher auch für einige der genutzten Drittbibliotheken auslaufen. Sollte in einer dieser Bibliotheken eine für die Anwendung relevante

Sicherheitslücke auftreten, steht keine unter Java 11 lauffähige Updateversion zur Verfügung.

- Die Unterstützung von Java 11 wird daher zum 30.04.2024 eingestellt.
- Sollte vor diesem Zeitpunkt eine für die Anwendung relevante Sicherheitslücke in einer Java 11-Bibliothek auftreten, wird die Unterstützung von Java 11 früher eingestellt.

7 Version 10.8.2

Veröffentlichung: 12.12.2023

Online-Update über den Installer

- Ein Online-Update der Version 10.8.0 auf Version 10.8.2 ist **möglich**.
- Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.7) zu verwenden.
- Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.
- **Signaturunterstützung auf Basis elliptischer Schlüssel:** Soft-Token, die mittels eins elliptischen Verfahrens erstellt worden sind, können nun zum Signieren verwendet werden
- **Geschwindigkeitsprobleme:** Es wurde ein Fehler behoben, der unter Umständen zu Geschwindigkeitsproblemen bei größeren PDF-Dokumenten geführt hat.
- **Zurücksetzen von Einstellungen auf Werkseinstellung**: Es wurde ein Fehler behoben, bei dem nicht alle veränderten Einstellungen auf Werkseinstellung zurückgesetzt wurden.
- **Einbindung der aktuellen Kartenansteuerung (MCard**) **2.11.0:** Mit dieser Version ist es möglich, die Karten des Anbieters D-Trust in der Version 5.1 und 5.4 zu erkennen.

8 Version 10.8.1

Veröffentlichung: 11.10.2023

Online-Update über den Installer

- Ein Online-Update der Version 10.8.0 auf Version 10.8.1 ist **möglich**.
- Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.7) zu verwenden.
- Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.3.4):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

Neue Validierungs-Features im Prüfprotokoll

- **Neue fachliche Prüfung für signierte PDF-Dateien**: Die bisherige (auch weiter so zur Verfügung stehende) fachliche PDF-Prüfung hat jegliche nachträgliche Änderung nach der zuletzt angebrachten Signatur bemängelt. Die neu hinzugefügte fachliche PDF-Prüfung bewertet die nachträglichen Änderung und stuft diejenigen Änderungen als sicher ein, die in Bezug zur Sicherheit und Vertrauenswürdigkeit der angebrachten Signaturen keine Auswirkungen haben können. Insbesondere werden nun nachträglich hinzugefügte Validierungsinformationen nicht mehr als Grund für ein Sicherheitsrisiko bewertet. Diese werden häufig durch Fernsignaturanbieter hinzugefügt.
- **Aktualisierter Algorithmenkatalog**: Nach Veröffentlichung des aktualisierten SOG-IS Katalogs wurden die darin aktualisierten Empfehlungen in den kombinierten Katalog der Governikus KG übernommen. Die prominenteste Aktualisierung ist die verlängerte Unterstützung des PKCS#1 v1.5 Signatur-Schemas bis Ende 2030. Der Algorithmenkatalog ist als Fallback in dem erstellten Artefakt enthalten.
- **Archive Cutoff**: Vertrauensdiensteanbieter können die Aussagekraft ihrer heraus gegebenen Sperrstatusinformationen zeitlich in die Vergangenheit beschränken. Dieses Datum nennt sich technisch "Archive Cutoff" und wird ab dieser Version in den HTML- und PDF-Prüfprotokollen angezeigt. Liegt der vermeintliche Signaturanbringungs-zeitpunkt vor diesem Datum, kann der Sperrstatusinformationen in Bezug zu der durchgeführten Signaturprüfung nicht vertraut werden. Grund ist das Verhindern einer potenziellen Falschpositivmeldung. Mit dieser Version wird das Archive Cutoff Datum in der Prüfung ignoriert, sofern die Sperrstatusantwort das beauskunftete Zertifikat als gesperrt ausweist. Dies liegt darin begründet, dass in diesem Fall keine Gefahr einer Falschpositivmeldung besteht.
- **Interpretation eingebetteter Validierungsinformationen**: Die in einer signierten Datei eingebetteten Sperrstatusinformationen werden ab sofort nur noch verwendet, sofern sich diese durch eine Prüfung für die Signaturvalidierung als geeignet erweisen. Bedingungen an die Geeignetheit sind zum Beispiel die Vertrauenswürdigkeit der ausstellenden Partei, die mathematische Gültigkeit der angebrachten Signatur auf den Sperrstatusinformationen und die Gültigkeit der dabei verwendeten Algorithmen sowie der geeignete zeitliche Zusammenhang mit dem Prüfzeitpunkt der eigentlich zu prüfenden Signatur (Sperrstatusinformation ist "frisch genug"). Sofern sämtliche eingebetteten Sperrstatusinformationen nicht geeignet sind, werden aktuelle online vom im Signaturzertifikat angegebenen Vertrauensdiensteanbieter eingeholt. Auf diesen Umstand wird im Prüfprotokoll verwiesen.

Fehlerbehebungen

- Verbesserungen im ZIP-Plug-in bei ZIP-Dateien mit nicht signierten Inhalten.
- Prüfverhalten bei D-Trust Zeitstempeln.
- SDI-Information werden fälschlicherweise aus den historischen Information der TL genutzt.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.
- **Prüfprotokoll**: Es wurde ein Fehler behoben, in dem das Prüfprotokoll nicht vollständig übersetzt wurde, wenn die Sprache auf Englisch eingestellt ist.
- **Leere HTTP Header:** Es wurde ein Fehler behoben, in dem leere HTTP-Header übermittelt wurden, wenn die Validierungsfunktion aufgerufen wurde.
- **Fehler in der Lizenzdatei:** Es wurde ein Fehler in der Bearbeitung des Parameters zur Schlüsselauswahl behoben.

9 Version 10.8.0

Veröffentlichung: 23.08.2023

Online-Update über den Installer

Ein Online-Update der Version 10.7.2 auf Version 10.8.0 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.7) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Öffnen von enveloped signierten Dateien**: Beim Öffnen einer enveloped signierten Datei innerhalb von Boreum, wird die Inhaltsdatei mit dem jeweiligen verknüpften Programm geöffnet.
- **Anbringung eines Signaturfeldes in ein gedrehtes PDF**: Eine PDF-Datei, die gedreht wurde, wurde nicht richtig erkannt, weswegen das Signaturfeld an einer falschen Position angebracht wurde.
- **Authentifizierungsproblem**: Es wurde ein Problem behoben, das unter Umständen beim Authentifizierungsdienst aufgetreten ist.
- **Bedienbarkeit**: Es wurden kleinere Anpassungen vorgenommen, um die Bedienbarkeit, insbesondere für die Barrierefreiheit, zu verbessern.
- **Prüfung von PDF-Dateien auf Passwortschutz:** Werden PDF-Dateien in Boreum zum Signieren hinzugefügt, die mit einem Passwortschutz versehen sind, wird ein entsprechender Hinweis ausgegeben.

10 Version 10.7.2

Veröffentlichung: 05.07.2023

Online-Update über den Installer

Ein Online-Update der Version 10.7.1 auf Version 10.7.2 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.7) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Zufallszahlenerzeugung:** Die Zufallszahlen werden über die von Java bereitgestellten Funktionen erzeugt, die eigens entwickelte Bibliothek wurde entfernt.
- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.3.1):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:
- **Fehlerbehebungen**:
  - Nebenläufiges Berechnen von Digest-Werten / SVR-Reports
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

11 Version 10.7.1

Veröffentlichung: 12.04.2023

Online-Update über den Installer

Ein Online-Update der Version 10.7.0 auf Version 10.7.1 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.7) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.3.0):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

  NEUE FEATURES

  - Aktualisierung an CAdES-Standard: 319 122-1 v1.2.1
  - Aktualisierung an XAdES-Standard: 319 132-1 v1.2.1

  FEHLERBEHEBUNGEN

  - Fehlendes Löschen der Temp-Files
  - Sinnvolles Abfangen von RunTimeExceptions

- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.
- **Umstellung auf QC-Statements**: Das Signaturniveau wird aus dem QC-Statement bezogen
- **Einbindung der aktuellen Kartenansteuerung (MCard**) **2.9.0:** Mit dieser Version ist es möglich, die Karten des Anbieters DGN zu erkennen.

12 Version 10.7.0

Veröffentlichung: 15.02.2023

Online-Update über den Installer

Ein Online-Update der Version 10.6.1 auf Version 10.7.0 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.7) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Verbesserung der PDF-A Konformität:** Behebung eines Fehlers, der dazu führte, dass beim Anlegen eines Signaturfeldes die PDF-A Konformität beeinträchtigt wurde.

- **Sichtbare PDF-Signaturen:** Umbenennung der Angabe „Unterzeichner:in“ in „Unterzeichnet von“.

- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.2.6):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

  FEHLERBEHEBUNGEN

  - Fehlerbehebung bzgl. Erkennung von "linearized"-Blöcken in PDF-Signaturdateien.
  - Es wurde eine Nullpointer-Exception behoben, welche bei Zertifikaten mit Seriennummer, die mit 9 Einsen anfängt, auftrat.
  - Delegierte OCSP-Responder müssen nach RFC 6960 die "Extended Key Usage" OCSPSigning aufweisen. Das wurde als Anforderungen nachgezogen.
  - Mehrere im Zertifikat hinterlegte OCSP-Responder werden nun erfolgreich durchiteriert, sofern der erste Responder keine verwertbare Antwort liefert.
  - Fehler bei nicht für Signatur zugelassenem Kryptoalgorithmus (ECIES) ist behoben und es wird eine entsprechende Fehlermeldung ausgegeben.
  - Es wurde eine Java Heap Exception behoben, welche durch fehlerhaftes Interpretieren von Validierungsdaten (OCSP-Responses, CRLs) innerhalb eines PDFs verursacht wurde.

  NEUE FEATURES

  - Bei nicht erfolgreicher OCSP-Einholung wird im Prüfprotokoll ausgegeben, welcher Responder hier angesprochen wurde und der HTTP-Fehlercode.

- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

13 Version 10.6.1

Veröffentlichung: 03.01.2023

Online-Update über den Installer

Ein Online-Update der Version 10.6.0 auf Version 10.6.1 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.5) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Verbesserung beim Laden von Signaturkarten:** Durch eine Umstellung in einer verwendeten Drittbibliothek kam es zu langen Ladezeiten beim Ansteuern von Signaturkarten bzw. Softwareschlüsseln. Diese lange Ladezeit wird mit dieser Version minimiert.

- **Verbesserung bei der Anzeige unter Windows 11:** Es wurden Verbesserungen bei der Größe der Anzeige vorgenommen, die maximale Anzeigegröße von Boreum ist auf die Bildschirmgröße begrenzt.

- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

Abkündigung der Unterstützung von Windows 8.1:

Mit der Folgeversion wird die Unterstützung von Windows 8.1 eingestellt, da der Herausgeber den Support zum 10. Januar 2023 einstellt.

14 Version 10.6.0

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 15.12.2022

Online-Update über den Installer

Ein Online-Update der Version 10.5.0 auf Version 10.6.0 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.5) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Unterstützung BNotK-Fernsignatur:** Es werden nun auch mehrere Schlüssel für eine:n Benutzer:in angezeigt und zur Auswahl angeboten, sollte diese:r mehrere zur Verfügung haben.
- **Sichtbare PDF-Signaturen:** Umbenennung der Angabe „Unterzeichner“ in „Unterzeichner:in“.
- **Umgang mit CVS-Zertifikaten:** Der Validierungsserver (Certificate Validation Server - CVS) erlaubt die Hinterlegung mehrerer Zertifikate, daher ist ein rechtzeitiger Austausch des Zertifikats nicht mehr notwendig.
  Nicht mehr benötigte Zertifikate, die nicht mehr im CVS hinterlegt sind, können gelöscht werden.
- **DATA Boreum IE:**
  - **Laden von SW-Schlüsseln:** Es wurde ein Fehler behoben, durch den das Laden eines Software-Schlüssels nicht richtig funktionierte und der Schritt der Schlüsselauswahl zum Teil nicht abgeschlossen werden konnte.
  - **Bereitstellung MultiClient 10.6.0:** Verbesserung im Umgang mit Groß- und Kleinschreibung (Für die Portvergabe verwendet der MultiClient USERNAME und CLIENTNAME in Großschreibung, z. B.: USERNAME=TESTER CLIENTNAME=RECHNERNAME01).
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.8.1:** Diese Version enthält eine Verbesserung in der Kartenerkennung für Bundesnotarkammer- und beA-Karten sowie die Unterstützung vom Betriebssystem macOS Ventura.
- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.2.3):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

  FEHLERBEHEBUNGEN
  - Beim Prüfen von detached Signaturen wurden temporär erzeugte Dateien nicht wieder gelöscht. Dies wurde nun behoben. Dies ist vor allem für den eCArd Service und für die Clients relevant.
  - Es wurde wegen eines CVEs die Batikversion auf 1.16 angehoben.

- Sobald der Signierzeitpunkt einer Signatur außerhalb des Gültigkeitsintervalls des Signaturzertifikats liegt (davor oder danach), wird dies angemerkt. Bisher wurde TOTAL_FAILED mit NOT_YET_VALID bzw. EXPIRED (Zeitpunkt vor Gültigkeitsintervall bzw. danach) zurück gegeben. Dies soll allerdings nur der Fall sein, wenn die Information "Signierzeitpunkt liegt außerhalb des Gültigkeitsintervalls" durch einen Zeitstempel (Content- oder Signaturzeitstempel) bewiesen vorliegt - dies wurde nun korrigiert. Ist die obige Information nur durch die Claimed Signing Time (CST) gestützt, so wird INDETERMINATE mit OUT_OF_BOUNDS_NO_POE zurückgegeben.
- PAdES-PlugIn: Bei PAdES-Signaturen wurde das Signaturzertifikat und die Zertifikatskette bisher ausschließlich aus dem PDF selbst entnommen und nicht aus der eingebetteten CMS-Signatur. Letzteres wird jetzt zusätzlich gemacht und hat Vorrang gegenüber der Zertifikatsquelle PDF. Damit sind jetzt auch Signaturen der Bundesagentur für Arbeit sinnvoll zu prüfen, welche auf einem Zertifikat beruhen, das keine Aussteller-Zertifikats-URL (Authority Information Access - caIssuers) bereit hält. Allerdings können diese Zertifikate alleinstehend ohne den Kontext einer Signaturprüfung nicht als qualifiziert geprüft werden.
- Es wurde ein Bug gefixt, der beim Validieren einer De-Mail Nachricht mit Output SVR auftrat.
- Kleinere Fehlerbehebungen beim Parsen von Signaturdateien.

NEUE FEATURES

- Übergabe Detached-Content CAdES-Signatur gemäß Anforderung.
- SMIME-PlugIn: Es werden nun auch signierte Mails unterstützt, die von Outlook 2019 exportiert wurden.
- PSD2/Open Banking-Erweiterung: Qualifizierte Zertifikate für elektronische Siegel oder Website-Authentifizierung können eine Erweiterung enthalten, in der zusätzlich Informationen zum Zahlungsdienstleister enthalten sind. Diese werden nun im menschenlesbaren Prüfprotokoll angezeigt.
- Optische Verbesserungen der menschenlesbaren Prüfprotokolle

- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

Abkündigung der Unterstützung von Windows 8.1:

Mit der Folgeversion wird die Unterstützung von Windows 8.1 eingestellt, da der Herausgeber den Support zum 10. Januar 2023 einstellt.

Mit dieser Version wird Windows 11 unterstützt.

Unterstützung macOS Ventura:

Mit dieser Version wird das aktuelle Apple Betriebssystem macOS Ventura unterstützt.

15 Version 10.5.0

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 01.09.2022

Online-Update über den Installer

Ein Online-Update der Version 10.4.0 auf Version 10.5.0 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.5) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Unterstützung des Fernsignaturdienstes der BNotK**: Die Bundesnotarkammer stellt ihr Angebot zur Anbringung von qualifizierten Signaturen auf eine Fernsignaturlösung, in Kombination mit Authentisierungskarten, um. Über DATA Boreum kann der Fernsignaturdienst angesprochen und mittels der lokalen Authentisierung eine qualifizierte Signatur erzeugt werden. Weitere Informationen entnehmen Sie bitte dem Anwendungshandbuch.
- **Proxyeinstellungen**: Behebung eines Fehlers beim Speichern der Proxyeinstellungen zum Validierungsdienst (CVS). Für die Online-Variante wurde der Fehler bereits behoben, mit dieser Bereitstellung erfolgt die Korrektur der Offline-Pakete für DATA Boreum.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.7.3**

16 Version 10.4.0

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 28.06.2022

Online-Update über den Installer

Ein Online-Update der Version 10.3.1 auf Version 10.4.0 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.4) zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Aktuelles .MSI (Installer) 3.0.4**: Bereitstellung eines neuen Installationsprogramms, mit dem eine verbesserte Darstellung der Anwendungsoberfläche auch bei höheren Bildschirmauflösungen möglich ist.
- **Umstellung auf Java 11:** Die Anwendung ist ab Version 10.4.0 ausschließlich lauffähig mit Java 11.
- **Mitgabe des zu nutzenden Zertifikats (DATA Boreum und DATA Boreum IE):** Es ist möglich, der Anwendung die Information mitzugeben, welches Zertifikat (Schlüsseldatei bzw. Hardwaretoken) zum Signieren zu verwenden ist. Die Mitgabe erfolgt über die Konfigurationsdatei (DATA Boreum) bzw. zusätzlich bei Hardwaretoken über einen Parameter (DATA Boreum IE). Informationen dazu finden Sie in den Entwicklungs- und Administrationshandbüchern.
- **Anbindung der DATA Deneb Services (Signaturdienst & Zeitstempeldienst):**
  - Unterstützung des BVSeal Fernsignaturdienstes (Anbindung über DATA Deneb)
  - Sind im Keycloak für einen Nutzenden mehrere Schlüssel zum Signieren (über den SignService) hinterlegt, werden alle Schlüssel zur Auswahl in DATA Boreum angezeigt (Tab Schlüsselauswahl)
  - Ab dieser Version liefert der SignService die Information an DATA Boreum, welches Schlüsselmaterial und welcher Algorithmus verwendet werden soll.
  - Unterstützung des Zugriffs unter Verwendung authentisierender Proxys.
- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.1.3):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

  NEUE FEATURES:
  - JAdES-PlugIn: Neues PlugIn zur Validierung von JAdES-profilierten JSON-Signaturen gemäß ETSI TS 119 182-1 (alle Baseline-Level).
  - Signaturen mit Signaturzertifikaten, welche die Short-Term-Erweiterung enthalten, werden standardmäßig unterstützt, falls eine der Governikus-Prüfrichtlinien verwendet wird. In diesem Fall wird auf das Einholen der Widerrufsinformation für das Short-Term-Signaturzertifikat verzichtet. Die Erweiterung besagt, dass der VDA zusichert, das Zertifikat während seines Gültigkeitszeitraums nicht zu sperren. Der Sperrstatus braucht daher nicht ermittelt zu werden und dieser Verzicht wird im Prüfprotokoll angezeigt.

- Inspection-Sheet HTML und PDF: Eine vorhandene Short-Term-Erweiterung in einem Signaturzertifikat wird in der Zertifikatsanzeige des Prüfprotokolls angezeigt.

FEHLERBEHEBUNGEN:

- Bei negativer Auskunft über den EU-Qualifikationsstatus eines Signaturzertifikats anhand einer hoheitlichen Vertrauensliste (EUMS-TL) wird diese nun auch als verwendete Vertrauensliste ausgegeben.
- Weitere kleine Fehlerbehebungen bei der Anzeige im Prüfprotokoll.
- Es wurde ein Sonderzeichen in den Zertifikatsdaten nicht korrekt escaped, was dazu führte, dass das PDF Prüfprotokoll nicht erstellt werden konnte. Dieser Fehler wurde behoben.
- Es wurden mögliche Quellen für nicht escapte Steuerzeichen ausgemacht und diese entsprechend behandelt. Der vorherige Zustand führte ggf. dazu, dass das PDF Prüfprotokoll nicht erstellt werden konnte.

- **Austausch der Informationen zum Validierungsdienst:** Über die Einstellungen ist es möglich, ein neues CVS-Zertifikat zu hinterlegen. Mit dieser Version wird ein Fehler behoben, der dazu führte, dass die Aktualisierung erst nach Neustart der Anwendung griff.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

Abkündigung der Unterstützung von Java 8:

Der Oracle-Support für Java 8 endete im März 2022.

Die Unterstützung von Java 8 wird daher mit Bereitstellung dieser Version 10.4.0 eingestellt.

Abkündigung Unterstützung 32-bit:

Ab dieser Version 10.4.0 werden ausschließlich 64-bit Umgebungen unterstützt.

17 Version 10.3.1

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 15.03.2022

Online-Update über den Installer

Ein Online-Update der Version 10.3.0 auf Version 10.3.1 ist **möglich**.

Es wird empfohlen, das aktuelle Installationsprogramm (.MSI, Version 3.0.2), welches mit dieser Version bereitgestellt wird, zu verwenden.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Anbindung der DATA Deneb Services (Signaturdienst & Zeitstempeldienst):** Mit dieser Version ändert erfolgt eine Abfrage von Benutzername und Passwort für die Authentisierung beim Zugriff auf den Signatur- und Zeitstempeldienst. Die Einstellung von Benutzername und Passwort über die Anwendung bzw. Konfigurationsdatei entfällt.
- **Verschlüsselung:** Korrektur bei der Auswahl eines Verschlüsselungszertifikats.
- **Einbindung der OSCI-Bibliothek 2.1.0**
- **Bereitstellung eines DATA Boreum MultiClients** für den Einsatz der DATA Boreum Integration Edition auf Terminalserverumgebungen.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.7.0:** Diese Version enthält die Unterstützung für Windows 11.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

	**Abkündigung der Unterstützung von Java 8:** Der Oracle-Support für Java 8 endet im März 2022. Die Unterstützung von Java 8 wird daher mit Bereitstellung der nächsten Version eingestellt. **Abkündigung Unterstützung 32-bit:** Mit der nächsten Version werden ausschließlich 64-bit Umgebungen unterstützt.

18 Version 10.3.0

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 27.01.2022

Online-Update über den Installer

Ein Online-Update der Version 10.2.0 auf Version 10.3.0 ist **möglich**.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Anbindung der DATA Deneb Services (Signaturdienst & Zeitstempeldienst):** Mit dieser Version ändert sich die Authentisierung zu den Services der Serverkomponente DATA Deneb. Die Authentisierung wird umgestellt auf den Standard OpenID Connect, welcher auf dem Autorisierungsframework OAuth2.0 basiert. Die neue Authentisierung wird ab der Bereitstellung der Governikus Suite 4.0.0 in DATA Deneb angeboten.
  Die Authentisierung erfolgt über Benutzername und Passwort, zusätzlich werden die Zugangsdaten für den im Authentisierungsdienst hinterlegten Client abgefragt (Client ID & Client Secret, zusätzlich der Realm-Name).
- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.0.3):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

  FEHLERBEHEBUNGEN:

  - PDF-Inspection-Sheet: Es wurde ein Problem beim Rendering des PDF-Prüfprotokolls behoben. Links aus Extensions in Zertifikaten mit Sonderzeichen führen nun nicht mehr zu einem Fehler beim Erstellen eines PDF-Prüfprotokolls.
- **Aktualisierung der verwendeten Drittbibliotheken**: Mit dieser Version wird unter anderem die Drittbibliothek log4j auf Version 2.17.1 aktualisiert. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

Abkündigung der Supportunterstützung von Java 8 in der Offline-Variante:

Die Anwendung ist lauffähig unter Java 8 und Java 11. Der Oracle-Support für Java 8 endet im März 2022.

Der Support von Java 8 wird daher auch für einige der genutzten Drittbibliotheken auslaufen. Sollte in einer dieser Bibliotheken eine für die Anwendung relevante Sicherheitslücke auftreten, steht keine unter Java 8 lauffähige Updateversion zur Verfügung.

Die Unterstützung von Java 8 wird daher zum 31.03.2022 eingestellt.

Sollte vor diesem Zeitpunkt eine für die Anwendung relevante Sicherheitslücke in einer Java 8-Bibliothek auftreten, wird die Unterstützung von Java 8 früher eingestellt.

19 Version 10.2.0

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 30.11.2021

Online-Update über den Installer

Ein Online-Update der Version 10.1.1 auf Version 10.2.0 ist **möglich**.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Change Requests:

- **CR 2020-05 Mehrfachsignatur:** Eine Datei (bspw. Musterschreiben.docx) kann von beliebig vielen Personen nacheinander detached signiert werden. Die Signaturen werden alle in einer Signaturdatei (bspw. Musterschreiben.docx.p7s) aufgenommen, vorausgesetzt, die Signaturdatei liegt im selben Ordner wie die Inhaltsdatei. Liegt die Signaturdatei in einem anderen Ordner als die Inhaltsdatei, die zum Signieren ausgewählt wird, wird mit dem Signaturvorgang eine neue Signaturdatei erstellt.

Verbesserungen und Fehlerbehebungen

- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.6.0:** Diese Version enthält im Vergleich zur Vorversion folgende Änderungen:
  - Unterstützung des neuen Betriebssystems macOS Monterey
  - Unterstützung des neuen barrierefreien Kartenlesegeräts Reiner SCT RFID komfort FON
  - Aktualisierung des Crypto-Provider auf die Version BC 1.69
- **Einbindung eines aktuellen Prüfprotokolls (CSL 3.0.1):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:

  UPDATE: Bouncy Castle auf Version 1.69, Apache Santuario XMLSec auf 2.2.3, Certificate Interpreter auf 1.16.3

  NEUE FEATURES:

  - Die Übergabe eines einzelnen End-Entity-Zertifikats (z.B. Signaturzertifikat) mit Übergabe eines Prüfzeitpunktes ist nun möglich. Die Anzeige der Prüfergebnisse ist in allen Protokollen (HTML, PDF, ETSI SVR [XML]) möglich. Angezeigt wird zusätzlich - neben dem Ergebnis der Gültigkeitsprüfung - der gewählte Prüfzeitpunkt und das Ergebnis der Ermittlung des Zertifikatniveaus und ggf. des Zertifikattyps. Die Meldungstexte wurden entsprechend ergänzt. Hinweis: Es können nur Zertifikate separat validiert werden, die nicht als Service Digital Identifier (SDI) in Vertrauens- listen konfiguriert sind und die nicht Root-Zertifikat (selbstsigniert) sind.
  - HTML- und PDF-Inspection-Sheets: Die Anzeige des Umfangs des Zertifikatsinhalts im HTML-/PDF-Prüfprotokoll ist nun über einen Parameter steuerbar. Als Default werden immer alle Inhalte angezeigt. Eine Kurzansicht zeigt nach Anforderung nur die Bereiche Inhaber, Aussteller, die Erweiterung QC-Statement und die wichtigsten Felder aus dem Bereich allgemeine

Angaben an. Bei Common-PKI-konformen Zertifikaten werden auch die beschränkenden Attribute aufgeführt.

- PDF-Inspection-Sheet: Navigation durch das PDF-Prüfprotokoll über verbessertes PDF-Inhaltsverzeichnis.
- SVR-Inspection-Sheet: Im ETSI-SVR sind die Meldungstexte (validation messages), sowie die ermittelten Niveaus von Signaturen und Zertifikaten nun als URIs angegeben, die auf (einem Governikus-Server) hinterlegte Meldungstexte und Niveaus referenzieren.
- XAdES-PlugIn: Unterstützt werden nun auch Baseline-Signaturen des Levels B bzw. BES gemäß TS V2.1.1 von 2012 und ETSI TS 101 903 V1.4.1 von 2009.

FEHLERBEHEBUNGEN

- Beim Mapping auf XKMS bei selbstsignierten End-Entity-Zertifikaten wird nun wieder zutreffend IndeterminateReason, IssuerTrust und RevocationStatus angezeigt.
- Kleinere Textkorrekturen bei der Anzeige von Prüfergebnissen im HTML- oder PDF-Prüfprotokoll.
- Die Prüfung des OCSP-Signer-Zertifikats erfolgt nicht mehr fälschlicherweise zu Existence sondern zu producedAt (Erstellungszeitpunkt der OCSP-Antwort angezeigt als CST-Wert).
- Die Kettenprüfung wird nun bei der Escape-Route (bei QES-Signaturen gemäß SigG Common-PKI-Spezifikation 2.0) auch dann ausgeführt, wenn die Schalenprüfung wegen eines abgelaufenen Zertifikats fehlschlägt.
- ASiC-PlugIn: Der Signaturtyp "Detached" wird in ASiC-Containern mit XAdES-Signatur nun erkannt.
- Drei fehlende Meldungstexte bei MinorIndication generic wurden ergänzt.

- **Einbindung des ETSI Signature Validation Reports (XML-Prüfprotokoll):** Über DATA Boreum können die Validierungsergebnisse u.a. in Form eines XML-Prüfprotokolls ausgegeben werden. Dieses XML-Prüfprotokoll ist ETSI konform (ETSI SVR XML-Prüfprotokoll), spezifiziert von ETSI in der EN 319 102-2, zurzeit als TS 119 102-2 in der Version 1.2.1 unterstützt.
- **Sichtbare Signaturfelder in PDF-Dokumenten:** Behebung eines Fehlers der dazu führte, dass beim Speichern von Signaturfeldern in PDF-Dokumenten diese an einer anderen Stelle, als ursprünglich platziert, gespeichert wurden.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

Abkündigung der Supportunterstützung von Java 8 in der Offline-Variante:

Die Anwendung ist lauffähig unter Java 8 und Java 11. Der Oracle-Support für Java 8 endet im März 2022.

Der Support von Java 8 wird daher auch für einige der genutzten Drittbibliotheken auslaufen. Sollte in einer dieser Bibliotheken eine für die Anwendung relevante Sicherheitslücke auftreten, steht keine unter Java 8 lauffähige Updateversion zur Verfügung.

Die Unterstützung von Java 8 wird daher zum 31.03.2022 eingestellt.

Sollte vor diesem Zeitpunkt eine für die Anwendung relevante Sicherheitslücke in einer Java 8-Bibliothek auftreten, wird die Unterstützung von Java 8 früher eingestellt.

20 Version 10.1.1

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 06.10.2021

Online-Update über den Installer

Ein Online-Update der Version 10.1.0 auf Version 10.1.1 ist **möglich**.

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **Sichtbare Signaturfelder in rotierenden PDF-Dokumenten:** Es wurde eine Verbesserung dahingehend eingebaut, dass sichtbare Signaturen auch in PDF-Dokumenten angebracht werden können, in denen der sichtbare Bereich durch eine Rotation um 90° verändert wurde.
- **PDF-Dokumente mit JPEG2000-komprimierten Grafiken:** Es wurde eine Verbesserung dahingehend eingebaut, dass Signaturfelder auch in JPEG2000-komprimierten PDF-Dokumenten angezeigt und für die Signatur verwendet werden können.
- **Löschen von Quelldateien:** Behebung eines Fehlers beim Löschen von Quelldateien beim Anbringen von PAdES – oder CAdES-Signaturen.
- **Einbindung eines aktuellen Prüfprotokolls (CSL 2.4.3):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:
  - PDF-PlugIn: Update auf Apache PDFBox 2.0.24 (Fix der CVE-2021-31811 und CVE-2021-31812).
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

An- und Abkündigungen

	**Abkündigung der Supportunterstützung von Java 8 in der Offline-Variante:** Die Anwendung ist lauffähig unter Java 8 und Java 11. Der Oracle-Support für Java 8 endet im März 2022. Der Support von Java 8 wird daher auch für einige der genutzten Drittbibliotheken auslaufen. Sollte in einer dieser Bibliotheken eine für die Anwendung relevante Sicherheitslücke auftreten, steht keine unter Java 8 lauffähige Updateversion zur Verfügung. **Die Unterstützung von Java 8 wird daher zum 31.03.2022 eingestellt.** Sollte vor diesem Zeitpunkt eine für die Anwendung relevante Sicherheitslücke in einer Java 8-Bibliothek auftreten, wird die Unterstützung von Java 8 früher eingestellt.

21 Version 10.1.0

Mit diesem Release wird erstmalig Governikus DATA Boreum als Integration Edition bereitgestellt.

Eine Übersicht zu den wichtigsten Änderungen gegenüber dem Governikus Signer entnehmen Sie bitte dem Dokument "Governikus DATA Boreum Integration Edition - Kurzinfo".

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 01.07.2021

Online-Update über den Installer

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Verbesserungen und Fehlerbehebungen

- **PDF Signatur - Angabe eines „Signaturortes“:** Die (optionale) Angabe eines Signaturortes erfolgt nicht mehr über Einstellungen -> PDF, sondern als Eingabe im Schritt „Optionen“. Wird ein Signaturort (ebenso wie ein Signaturgrund) angegeben, wird diese Information sowohl in sichtbaren Signaturen als auch unsichtbaren Signaturen von pdf-Dokumenten übernommen und dargestellt.
- **Behebung eines Fehlers beim Laden der Proxy-Einstellungen aus dem System**.
- **PIN-Eingabe:** Mit dieser Version erfolgt die PIN-Eingabe standardmäßig über das Kartenlesegerät. Ist die PIN-Eingabe über die Tastatur des PCs gewünscht, kann dies über eine Ergänzung in der .ini-Datei der Anwendung eingestellt werden (Erklärung siehe Dokument „ReadMe Governikus Signer PIN-Eingabe“).
- **Einbindung eines aktuellen Prüfprotokolls (CSL 2.4.2):** Mit dieser Version werden folgende Änderungen zur Vorversion umgesetzt:
    - PDF-PlugIn: Es wird nun ein vollständig PDF-UA-konformes Prüfprotokoll (PAC 3 getestet) mit einigen Warnungen erzeugt.
    - Bei der Prüfung der Signatur der CVP-Antwort des Certificate Validation Servers wurde die Fehlerbehandlung verbessert. Es wird nun vorab geprüft, ob die HTTP-Response Daten oder einen Fehlercode enthält.
    - Der Ermittlungsalgorithmus der Eignung einer Custom-TL/Governikus-TL wurde so ergänzt, dass nun auch Meldungstexte angezeigt werden, wenn die verwendete TL abgelaufen oder nicht gültig signiert ist und daher den angezeigten Inhalten aus der TL (Niveau und Typ der Signatur) nicht vertraut werden darf. Das Niveau wird dann zutreffend nur auf digitale Signatur gesetzt.
    - PDF-PlugIn: Die unvollständige Implementierung eines Stream-Readers konnte dazu führen, dass die mathematische Signaturprüfung in seltenen Fällen fälschlich misslang. Der Fehler wurde behoben.
    - PDF-PlugIn: Die Revisionsangabe erfolgt nun wieder korrekt vor dem letzten Punkt des PDF-Dateinamens.
    - Validierungsalgorithmus: Wird eine Signatur validiert, ohne dass ein CVS konfiguriert wurde (oder eine falsche URL) konfiguriert wurde wird jetzt zutreffend (wie bei abgeschalteter Zertifikatsprüfung über das System oder eine Custom-Policy) der Gesamtstatus maximal indeterminate. In allen Fällen wird

nun ein entsprechender Meldungstext für die Ursache des Unbestimmt-Status angezeigt.

- XKMS-Mapping: Ein Fehler beim Mapping vom CVP- auf den XKMS-Report wurde gefixt. Bei einem selbstsigniertes EE-Zertifikat führt das Mapping auf XKMS jetzt zutreffend immer zu „IndeterminateReason“ IssuerTrust und RevocationStatus.
- SVR-PlugIn: Ein Fehler bei der Erstellung des SVR-Report bei validierten OSCI-Nachrichten mit signierten Attachments wurde behoben. Es wird jetzt für die Signaturen der geprüften signierten Dokumente für den SignatureValidationStatus eine mainindication TOTAL-PASSED oder INDETERMINATE oder TOTAL-FAILED angezeigt.
- InspectionSheet-PlugIn: Soweit vorhanden wird nun immer der Signaturgrund und/oder der Signaturort bei PAdES-Signaturen angezeigt.
- HTML- und PDF-PlugIn: Umlaute werden wieder korrekt dargestellt.
- Ein Fehler bei der Ermittlung der Vertrauensstellung von CRL bei der Verwendung der Governikus-TL oder Custom-TLs wurde behoben. Die Stellung kann nun immer korrekt ermittelt werden.
- SVR-PlugIn: Die Erzeugung der CryptoInformation Objekte war nicht chemakonform. ValidationObjectIds werden nun erzeugt.
- SVR-PlugIn: Wird für eine Signatur ECDSA benutzt, dann wurde bisher das CryptoInformation Objekt ungültig da das SVP-Protokoll keine URI enthält. Als alternative URI-Darstellung wird nun eine OID genutzt.
- SVR-PlugIn: Wird bei der Validierung die Zertifikatprüfung abgeschaltet, so ergibt sich beim Erstellen des SVR keine NPE mehr, weil der NonValidatingCertValidator die Felder für den Zertifikat-Signaturalgorithmus, das Best POE-Datum und den POE-Typ in der CSL-Response nicht mehr füllen kann. Da diese SVR-Knoten aber nur optional sind, wurde deren Erstellung unterbunden, wenn sie keine Daten enthalten.

- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.5.7:** Diese Version enthält im Vergleich zur Vorversion folgende Änderungen:
  - Diese Version der MCard wurde um den GCM-Support für die CMS-Entschlüsselung erweitert. Es werden nun die Entschlüsselungsmethoden CBC und GCM unterstützt.
- **Aktualisierung der verwendeten Drittbibliotheken**: Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.

22 Version 10.0.0

Mit diesem Release wird erstmalig Governikus DATA Boreum, das Nachfolgeprodukt zum Governikus Signer, bereitgestellt. Die Installation von DATA Boreum erfolgt unabhängig vom Governikus Signer.

Eine Übersicht zu den wichtigsten Änderungen gegenüber dem Governikus Signer entnehmen Sie bitte dem Dokument "Governikus DATA Boreum - Kurzinfo".

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Veröffentlichung: 14.04.2021

Online-Update über den Installer

Die im Installationsprogramm mitgelieferte Java-Version ist OpenJDK Version 11.

Change Requests:

- **CR 2017-06 Umstellung auf eIDAS-Komponenten:** Ersatz der bisherigen Kryptobibliotheken durch die neue eIDAS-konforme CryptoService Library (CSL), die alle relevanten ETSI-EN/technischen Standards erfüllt. Voraussetzung ist der serverseitige Einsatz von Governikus DATA Varuna (CVS).
- **CR 2020-07 Umstellung auf OpenJDK:** Mit dieser Bereitstellung erfolgt ein Wechsel von Oracle Java zu OpenJDK11.
- **CR 2019-06 Umsetzung von Anforderungen an die Barrierefreiheit**: Mit dieser Version werden die grundlegenden Anforderungen an eine barrierefreie Ausgestaltung der Anwendung umgesetzt. Weitere Anpassungen folgen bzw. werden fortlaufend mit der Softwareweiterentwicklung vorgenommen.

Verbesserungen und Fehlerbehebungen

- **Einbindung eines aktuellen Prüfprotokolls (CSL 2.3.1):** Mit dieser Version wird ein überarbeitetes, eIDAS-konformes Prüfprotokoll bereitgestellt.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.5.4:** Diese Version enthält folgende Besonderheiten:
  - Diese Version beinhaltet Änderungen an der PC/SC-Ansteuerung, die zu einer verbesserten Neuerkennung von angeschlossenen Kartenlesern in einer Terminalserver-Umgebung führt.
  - Es wurden Anpassungen für die ScreenReader-Funktionalität des Standard-Pin-Dialogs vorgenommen (Auslesen von Labels und Erläuterungstexten).
- **Aktualisierung der verwendeten Drittbibliotheken**. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus DATA Boreum Nutzungsbedingungen" entnehmen.