

Governikus KG



Governikus

Communicator

Release-Übersicht

Governikus Communicator Justiz Edition

Governikus Communicator Justiz Edition 3.7.8.0

© 2020 Governikus GmbH & Co. KG

Inhaltsverzeichnis

1	Version 3.7.8.0.....	3
2	Version 3.7.7.1.....	4
3	Version 3.7.7.0.....	6
4	Version 3.7.6.0.....	8
5	Version 3.7.5.2.....	10
6	Version 3.7.5.1.....	11
7	Version 3.7.5.0.....	12
8	Version 3.7.4.0.....	14
9	Version 3.7.3.2.....	15
10	Version 3.7.3.1.....	16
11	Version 3.7.3.0.....	17
12	Version 3.7.2.3.....	18
13	Version 3.7.2.2.....	20
14	Version 3.7.2.1.....	22
15	Version 3.7.2.0.....	24
16	Version 3.7.1.0.....	26

1 Version 3.7.8.0

30.04.2020 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.8.7
MCard (Kartenansteuerung):	Version 2.4.0
Certificate Interpreter (CI):	Version 1.15.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.14.0
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.9.0
Algorithmenkatalog:	Version 2019
Bouncy Castle:	Version 1.64

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.7.1 auf Version 3.7.8.0 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.8 (inkl. Oracle JRE 8 Update 201) zur Nutzung zur Verfügung.

Verbesserungen:

- **Änderung der zugelassenen Zeichen in Dateinamen:** In Dateinamen von Anhängen dürfen nun auch die Umlaute ä, ö und ü sowie ß genutzt werden. Dies wurde nachträglich zum ursprünglichen Beschluss der BLK AG IT-Standard der Justiz geändert und als Anforderung an Drittprodukte im EGVP veröffentlicht (siehe www.egvp.de).
- **Senden an E-Malempfänger (Nachrichten/Anhänge) und Debug-Modus:** Die über das Kontextmenü einer OSCI-Nachricht erreichbare Funktion "Senden an E-Mail-Empfänger..." kann auf Systemen mit 64-Bit-Java derzeit keine Anhänge und Nachrichten über ein Standard-E-Mail-Programm versenden. Diese Einschränkung betrifft auch den Debug-Modus. Das Versenden erfolgt daher direkt aus der Anwendung heraus. Für das Versenden ist es erforderlich, dass der Nutzer einmalig seine E-Mail-Adresse sowie den Namen und Port des verwendeten SMTP-Servers angibt. Für Windows-Nutzer, die Outlook als E-Mailprogramm verwenden, wird mit dieser Version die Möglichkeit geschaffen, dies auch für den Versand von Nachrichten, Anhängen und Debug-Logdateien aus der Anwendung heraus zu verwenden. Voraussetzung dafür ist, dass EML-Dateien im System mit Outlook verknüpft werden.

2 Version 3.7.7.1

20.02.2020 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.7.7
MCard (Kartenansteuerung):	Version 2.4.0
Certificate Interpreter (CI):	Version 1.15.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.14.0
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.9.0
Algorithmenkatalog:	Version 2019
Bouncy Castle:	Version 1.64

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.7.0 auf Version 3.7.7.1 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.8 (inkl. Oracle JRE 8 Update 201) zur Nutzung zur Verfügung.

Verbesserungen:

- **Einbindung des aktuellen Prüfprotokolls 3.14.0** (Verification Interpreter): Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtigen Änderungen:
 - Aktualisierung des Algorithmenkatalogs 5.3.0.: Legacy-Algorithmen aus dem SOG-IS-Katalog werden nun gemäß Empfehlung der BNetzA bis zum angegebenen Datum als vollumfänglich geeignet für eine QES angesehen.
- **Einbindung der aktuellen OSCI-Bibliothek 1.9.0:**
 - Verwendung von AES-256-GCM anstelle von AES-256-CBC als Standardmodus für die symmetrische Verschlüsselung
 - Verwendung von RSA-OAEP anstelle von RSAES-PKCS1-v1_5 als Standardmodus für die asymmetrische Verschlüsselung
- **Aktualisierung von verwendeten Drittbibliotheken:** Es wurde mehrere Drittbibliotheken aktualisiert. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Justiz Edition Nutzungsbedingungen" entnehmen.
- **Verbesserungen bei der Nutzung mehrerer Monitore:** Beim Verwenden von mehreren Monitoren wird die Anwendung immer auf dem Hauptmonitor angezeigt. Damit wird verhindert, dass die Anwendung bei Änderungen der verwendeten Monitore im „unsichtbaren“ Bereich angezeigt wird.
- **Aktualisieren der Favoritenliste:** Wenn beim Synchronisieren des Adressbuchs eine SAFE-Instanz nicht erreichbar ist, wird derzeit davon ausgegangen, dass die

zugehörigen Einträge nicht mehr vorhanden sind. Diese werden aus den Favoriten gelöscht. Zukünftig wird bei Nichterreichbarkeit einer SAFE-Instanz die Synchronisation abgebrochen und diese Nutzer nicht aus den Favoriten gelöscht.

- **Umgang mit Vertretern in den Favoriten:** Derzeit wird ein Eintrag in der Favoritenliste auf eine neue SAFE-ID aktualisiert, wenn ein Vertreter eingetragen wird. Zukünftig wird ein Eintrag in der Favoritenliste nur aktualisiert, wenn kein Vertreter auf SAFE eingetragen ist. Auf SAFE eingetragene Vertreter erhalten die Nachrichten trotzdem.

3 Version 3.7.7.0

04.12.2019 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.7.0
MCard (Kartenansteuerung):	Version 2.4.0
Certificate Interpreter (CI):	Version 1.15.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.13.0
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle:	Version 1.64

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.6.0 auf Version 3.7.7.0 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.8 (inkl. Oracle JRE 8 Update 201) zur Nutzung zur Verfügung.


Change Requests:

- **CR 2019-10 „GovCom: Verteilerlisten“:** Mit dieser Version ist es möglich, lokale Verteilerlisten für den Nachrichtenversand an mehrere Empfänger einzurichten und zu nutzen.
- **CR 2019-16 „GovCom: Notwendige Erweiterungen für den Einsatz im EGVP-System“:** Entsprechend eines Beschlusses der BLK-AG IT-Standards werden die Länge und die verwendeten Zeichen in Dateinamen von Anhängen ab 01.01.2020 beschränkt. Der Beschluss ist bindend für alle zugelassenen OSCI-Drittprodukte im EGVP-System:
 - Die Länge von Dateinamen wird auf max. 90 Zeichen (inkl. Dateiendung) beschränkt. Die Dateinamen dürfen nicht abgeschnitten oder in sonstiger Weise verändert werden.
 - In Dateinamen dürfen nur noch alle Buchstaben des deutschen Alphabetes bis auf die Umlaute ä, ö, ü und ß genutzt werden. Zudem dürfen alle Ziffern und die Zeichen Unterstrich und Minus genutzt werden. Punkte sind nur als Trenner zwischen Dateiname und Dateinamenserweiterung zulässig. Nur bei konkatenierten Dateinamenserweiterungen, z.B. bei abgesetzten Signaturdateien, dürfen Punkte auch im Dateinamen genutzt werden (z.B. Dokument1.pdf.pkcs7).

Verbesserungen:

- **Einbindung des aktuellen Prüfprotokolls 3.13.0** (Verification Interpreter): Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtigen Änderungen:
 - Aktualisierung verwendeter Drittbibliotheken.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.4.0:** Diese Version enthält im Vergleich zur Vorversion folgende Änderungen:
 - Es wird der Chipkartenleser Cyberjack one von Reiner SCT und die Cherry-Tastatur KC 1000 SC-Z mit integriertem Chipkartenleser der Sicherheitsklasse 2 für die Nutzung mit Windows unterstützt.
- **Aktualisierung von verwendeten Drittbibliotheken:** Es wurde mehrere Drittbibliotheken aktualisiert. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Justiz Edition Nutzungsbedingungen" entnehmen.

An-/Abkündigungen:

	<p>Abkündigung Windows 7:</p> <p>Microsoft hat angekündigt, ab dem 14. Januar 2020 keine Sicherheitsupdates mehr für Windows 7 zur Verfügung zu stellen. Der Support durch Microsoft wird dann ebenfalls eingestellt. Dieser Umstand kann die für eine Signaturanwendungskomponente geforderte hohe Sicherheit gegen potenzielle Bedrohungen beeinträchtigen.</p> <p>Windows 7 wird daher ab diesem Zeitpunkt nicht mehr unterstützt.</p>
--	--

4 Version 3.7.6.0

30.10.2019 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.6.0
MCard (Kartenansteuerung):	Version 2.2.5
Certificate Interpreter (CI):	Version 1.14.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.11
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle:	Version 1.64

Online-Update über den MSI-Installer:


Ein Online-Update der Version 3.7.5.2 auf Version 3.7.6.0 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.5 zur Nutzung zur Verfügung.

Verbesserungen:

- **Umstellung auf den GC-Betriebsmodus für die Inhaltsdatenverschlüsselung:** Aufgrund der Festlegung im Standard XInneres inklusive seiner Module (XMeld, XAusländer, XPersonenstand und Basismodul), dass ab 1.11.2019 für die Inhaltsdatenverschlüsselung ausschließlich AES-GCM zu verwenden ist (siehe <https://www.xoev.de/downloads-2316>), erfolgt die Umstellung der Inhaltsdatenverschlüsselung auf den GC-Betriebsmodus ebenfalls im Governikus Communicator Justiz Edition.
- **Aktualisierung von verwendeten Drittbibliotheken:** Es wurde mehrere Drittbibliotheken aktualisiert. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Justiz Edition Nutzungsbedingungen" entnehmen.

An-/Abkündigungen:

	<p>Abkündigung Windows 7:</p> <p>Microsoft hat angekündigt, ab dem 14. Januar 2020 keine Sicherheitsupdates mehr für Windows 7 zur Verfügung zu stellen. Der Support durch Microsoft wird dann ebenfalls eingestellt. Dieser Umstand kann die für eine Signaturanwendungskomponente geforderte hohe Sicherheit gegen potenzielle Bedrohungen beeinträchtigen.</p> <p>Windows 7 wird daher ab diesem Zeitpunkt nicht mehr unterstützt.</p>
---	--

5 Version 3.7.5.2

27.08.2019 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.5.5
MCard (Kartenansteuerung):	Version 2.2.5
Certificate Interpreter (CI):	Version 1.14.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.11
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle:	Version 1.62

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.5.1 auf Version 3.7.5.2 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.5 zur Nutzung zur Verfügung.

Verbesserungen:

- **Änderung in der Kommunikation zum OSCI-Manager:** Es wurde festgestellt, dass derzeit keine neuen Postfächer auf dem Verfahrensbeteiligten-Intermediär angelegt werden können. Bis zur abschließenden Analyse der Ursache wird eine Änderung in der Client-Anwendung vorgenommen, um dies wieder zu ermöglichen.

6 Version 3.7.5.1

21.08.2019 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.5.4
MCard (Kartenansteuerung):	Version 2.2.5
Certificate Interpreter (CI):	Version 1.14.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.11
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle:	Version 1.62

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.5.0 auf Version 3.7.5.1 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.5 zur Nutzung zur Verfügung.

Fehlerbehebungen:

- **Fehler beim Abholen mehrerer Nachrichten vom OSCI-Manager:** Ein Fehler in der Kommunikation zwischen OSCI-Manager und Client-Anwendung hat zur Folge, dass beim Abholen mehrerer Nachrichten nur die erste erfolgreich abgeholt werden kann. Dieser Fehler wurde korrigiert.

7 Version 3.7.5.0

20.08.2019 (Produktiv)

Basissysteme:

Governikus Communicator Framework:	Version 3.7.5.2
MCard (Kartenansteuerung):	Version 2.2.5
Certificate Interpreter (CI):	Version 1.14.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.11
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle:	Version 1.62

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.4.0 auf Version 3.7.5.0 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.5 zur Nutzung zur Verfügung.

Verbesserungen und Fehlerbehebungen:

- **Einbindung des aktuellen Prüfprotokolls** (Verification Interpreter) 3.10.11: Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtige Änderung:
 - PadES-PlugIn: Aktualisierung der Apache PDFBox auf Version 2.0.15.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.2.5:** Diese Version enthält im Vergleich zur Vorversion folgende Änderungen:
 - Die Omnikey-Leser 3x21 wurden aus der Unterstützung entfernt, weil die Geräte ihr End-of-Life-Zyklus erreicht haben. Vom Hersteller werden keine Sicherheitsupdates oder Treiber mehr bereitgestellt.


Informationen zu unterstützten Karten, Lesegeräten und Betriebssystemen finden Sie im Dokument "Unterstützte Kombinationen Leser-Karten-Betriebssysteme".

- **Aktualisierung von verwendeten Drittbibliotheken:** Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Justiz Edition Nutzungsbedingungen" entnehmen.
- **Erweiterung der Funktionalität zum Versand und Empfang großer Nachrichten (Fortführung „EFFI“ um dynamisches Aushandeln der „Chunk“-Größen):** Die Anwendung ist bereits seit längerem auf den Versand und Empfang großer Nachrichten vorbereitet (s. CR 2017-04 Umgang mit großen Nachrichten). Mit dieser Version erfolgt eine Erweiterung des Funktionsumfangs dahingehend, dass die

Anwendung beim Versand und Empfang von Nachrichten am OSCI-Manager abfragt, ob dieser eine Konfiguration der Chunk-Größen vorgenommen hat (Min. und Max. Werte). Hat der OSCI-Manager keine Werte eingetragen oder liegt die Chunk-Größe der Anwendung innerhalb des konfigurierten Wertes, wird der Chunk-Wert der Anwendung verwendet. Liegt der Chunk-Wert der Anwendung unterhalb des Wertes des OSCI-Managers, wird der Minimalwert des OSCI-Managers verwendet. Liegt der Chunk-Wert der Anwendung oberhalb des Wertes des OSCI-Managers, wird der Maximalwert des OSCI-Managers verwendet. Die Standard-Chunkgröße der Anwendung beträgt 20MB.

- **Verbesserung bei der Nutzung von Authentisierung über Proxy-Pac-Dateien:** Kommt es bei der Authentisierung an einem Proxy zu einem Timeout, wird eine Fehlermeldung angezeigt und die Anwendung beendet.
- **Verbesserung der Lesbarkeit:** Während der Tests der Version 3.7.5.0 wurde festgestellt, dass sich die Darstellung der Schriftgröße mit aktuellen Java-Versionen verschlechtert hat, so dass die Beschriftungen zum Teil schwer lesbar waren. Daher wird der Anwendung fortan eine feste Schriftart (Verdana) sowie Schriftgröße (12) vorgegeben.

An-/Abkündigungen

	<p>Abkündigung Windows 7:</p> <p>Microsoft hat angekündigt, ab dem 14. Januar 2020 keine Sicherheitsupdates mehr für Windows 7 zur Verfügung zu stellen. Der Support durch Microsoft wird dann ebenfalls eingestellt. Dieser Umstand kann die für eine Signaturanwendungskomponente geforderte hohe Sicherheit gegen potenzielle Bedrohungen beeinträchtigen.</p> <p>Windows 7 wird daher ab diesem Zeitpunkt nicht mehr unterstützt.</p>
---	--

8 Version 3.7.4.0

Bereitstellung: 30.04.2019

Basissysteme:

Governikus Communicator Framework:	Version 3.7.4.0
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.13.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.10
Transportschicht (http-Transport):	Version 2.4.0.19
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle:	Version 1.61

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.3.2 auf Version 3.7.4.0 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.5 zur Nutzung zur Verfügung.

Verbesserungen und Fehlerbehebungen:

- **Aktualisierung von verwendeten Drittbibliotheken:** Es wurde die Bibliotheken pdfbox (Version 2.0.13) und Bouncy Castle (1.61) aktualisiert. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Justiz Edition Nutzungsbedingungen" entnehmen.
- **Verbesserung beim Fachdatenimport:** Wurde der Import einer Nachricht unterbrochen, werden nicht vollständig importierte Fachdaten beim Öffnen des Postfachs gelöscht, damit keine unvollständigen („roten“) Nachrichten im Postausgang liegen.
- **Verbesserung bei Proxyauthentisierung und Timeout:** Kommt es bei der Authentisierung an einem Proxy zu einem Timeout, „friert“ die Anwendung nicht mehr ein.
- **Einbindung des aktuellen Prüfprotokolls** (Verification Interpreter) 3.10.10: Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtigen Änderungen:
 - Verbesserung der Erkennung von Fehlern in der Strukturprüfung von PDF-Inline-Signaturen.
 - Behebung eines Fehlers bei der Verarbeitung leerer OSCI-Nachrichten.

Informationen zum Governikus-Prüfprotokoll finden Sie im Dokument "Anwenderhandbuch Governikus-Prüfprotokoll".

9 Version 3.7.3.2

Bereitstellung: 17.12.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.3.3
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.12.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.7
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.60

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.3.1 auf Version 3.7.3.2 ist **möglich**.

Es steht ein MSI-Installer in Version 2.0.5 zur Nutzung zur Verfügung.

Verbesserungen und Fehlerbehebungen:

- **Nutzung des RSA OAEP-Paddingalgorithmus für die Inhaltsdatenverschlüsselung:** Da das Padding-Verfahren RSA PKCS#1-v1.5 als auslaufend gemäß SOG-IS gilt und vom BSI nicht mehr empfohlen wird, wird die Verschlüsselung der Inhaltsdaten nun mit dem aktuell empfohlenen Algorithmus RSA OAEP durchgeführt. Der Empfang und die Verarbeitung von Nachrichten, die noch mit dem Padding-Verfahren RSA PKCS#1-v1.5 verschlüsselt wurden, ist weiterhin möglich.

10 Version 3.7.3.1

Bereitstellung: 03.12.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.3.2
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.12.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.7
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.3
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.60

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.3.0 auf Version 3.7.3.1 ist **möglich**.

Es muss ein MSI-Installer ab Version 2.0.2 verwendet werden.

Verbesserungen und Fehlerbehebungen:

- **Einbinden der aktuellen OSCI-Bibliothek 1.8.3**
- **Einbindung des aktuellen Prüfprotokolls (Verification Interpreter) 3.10.7:** Die Aktualisierung erfolgt aufgrund technisch notwendiger Anpassungen für die Nutzung der OSCI-Bibliothek in der aktuellen Version 1.8.3.
- **Weiterleiten einer Nachricht per E-Mail:** Beim „Weiterleiten einer Nachricht per E-Mail“ wird nun neben der Nachrichten-ID auch der ursprüngliche Betreff aus der Nachricht als E-Mail Betreff übernommen.
- **Verbesserung im Umgang mit Suchergebnissen aus SAFE:** Bei der Suchanfrage zu einem Nutzer erwartet der Client die Lieferung bestimmter Parameter, wie Organisation, Rolle etc. Da nicht alle SAFE-konformen Verzeichnisdienste diese Parameter zwingend zurückgeben, wurden einige Parameter im Client als optional eingestuft, damit eine fehlerhafte Anzeige von Suchergebnissen vermieden wird (konkret: das Objekt „EJusticeAttributesType“ (liefert Organisation, Organisationseinheit und Rollenwert/Typ) wird als optional behandelt).

11 Version 3.7.3.0

Bereitstellung: 30.10.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.3.0
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.12.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.1
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.1
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.60

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.2.3 auf Version 3.7.3.0 ist **möglich**.

Es muss ein MSI-Installer ab Version 2.0.1 verwendet werden.

	<p>Nutzung des aktuellen MSI-Installers Version 2.0.2:</p> <p>Für die <u>produktive</u> Umgebung steht der MSI-Installer Version 2.0.2 bereit. Ab dieser Version werden die Anwendungsressourcen abgesichert über https vom Downloadserver der Governikus KG heruntergeladen.</p> <p>Bitte beachten Sie, dass ältere MSI-Installerversionen als die Version 2.0.2 nur bis zum 2. November 2018 verwendet werden können. Stellen Sie daher rechtzeitig auf die neue Version um.</p>
---	--

Verbesserungen und Fehlerbehebungen:

- **Umgang mit Sonderzeichen in Dateianhangsnamen:** Die derzeit zulässigen Sonderzeichen in Dateianhangsnamen finden sich in der Dokumentation. Mit dieser Version erfolgt eine Prüfung beim Erstellen einer neuen Nachricht über das Nachrichtenfenster oder über die Fachdatenschnittstelle dahingehend, ob in den Dateianhängen nicht zulässige Zeichen vorhanden sind. Ist dies der Fall, kann ein Anhang einer Nachricht nicht hinzugefügt werden. Dem Nutzer wird in diesem Fall eine entsprechende Fehlermeldung angezeigt.
- **Behebung eines Fehlers im Umgang mit Proxyeinstellungen:** Die Einstellungen zum Proxy, die über die Anwendung vorgenommen werden, sollen beibehalten und nicht durch die Systemeinstellungen überschrieben werden.

12 Version 3.7.2.3

Bereitstellung: 17.09.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.2.9
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.12.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.1
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.1
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.60

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.2.2 auf Version 3.7.2.3 ist **möglich**.

Es muss ein MSI-Installer ab Version 2.0.1 verwendet werden.

	<p>Nutzung des aktuellen MSI-Installers Version 2.0.2:</p> <p>Für die <u>produktive</u> Umgebung steht der MSI-Installer Version 2.0.2 bereit. Ab dieser Version werden die Anwendungsressourcen abgesichert über https vom Downloadserver der Governikus KG heruntergeladen.</p> <p>Bitte beachten Sie, dass ältere MSI-Installerversionen als die Version 2.0.2 nur bis zum 2. November 2018 verwendet werden können. Stellen Sie daher rechtzeitig auf die neue Version um.</p>
---	--

Verbesserungen und Fehlerbehebungen:

- **Teilweise Umstellung auf den GC-Modus (Galois/Counter Mode)*:** Für den Verschlüsselungsalgorithmus AES empfehlen sowohl das W3C als auch das BSI aus Sicherheitsgründen den Einsatz des Betriebsmodus GCM vorrangig vor dem CBC-Modus (siehe <https://www.xoev.de/downloads-2316>). Daher ist eine Umstellung auf den aktuell empfohlenen Betriebsmodus GCM ebenfalls im Governikus Communicator notwendig.
Die Kommunikation mit dem OSCI-Manager (die Transportverschlüsselung des "äußeren Umschlags" beim Senden und Empfangen von Nachrichten, Abholen von

* Galois/Counter Mode (GCM) ist ein Betriebsmodus, in dem Blockchiffren für eine symmetrische Verschlüsselungsanwendung betrieben werden können. Informationen zum empfohlenen Umstieg siehe u.a. <https://www.xoev.de/downloads-2316>.

Laufzetteln, E-Mail-Benachrichtigung u.w.) wird ab dieser Version auf den GC-Betriebsmodus umgestellt. Ebenso kann der Governikus Communicator ab dieser Version OSCI-Nachrichten empfangen, die mit dem GC-Modus verschlüsselt wurden. Die Umstellung auf den GC-Modus für die Verschlüsselung von Nachrichten (Verschlüsselung des "inneren Umschlags") beim Versand erfolgt mit einer späteren Version, da diese in Abstimmung mit anderen OSCI-Transport-Produkten erfolgen muss.

- **Verbesserung beim Starten des Governikus Communicators außerhalb des sichtbaren Bereichs:** Wird bspw. ein genutzter zweiter Monitor entfernt, startet der Governikus Communicator nun im sichtbaren Bereich des genutzten ersten Monitors.
- **Aktualisierung von verwendeten Drittbibliotheken:** Es wurden die Bibliotheken commons-compress 1.18 sowie log4j 2.11.1 aktualisiert. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Nutzungsbedingungen" entnehmen.

13 Version 3.7.2.2

Bereitstellung: 16.08.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.2.4
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.12.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.1
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.1
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.60

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.2.1 auf Version 3.7.2.2 ist **möglich**.

Es muss ein MSI-Installer ab Version 2.0.1 verwendet werden.

	<p>Nutzung des aktuellen MSI-Installers Version 2.0.2:</p> <p>Für die <u>produktive</u> Umgebung steht der MSI-Installer Version 2.0.2 bereit. Ab dieser Version werden die Anwendungsressourcen abgesichert über https vom Downloadserver der Governikus KG heruntergeladen.</p> <p>Bitte beachten Sie, dass ältere MSI-Installerversionen als die Version 2.0.2 nur bis zum 2. November 2018 verwendet werden können. Stellen Sie daher rechtzeitig auf die neue Version um.</p>
---	--

Verbesserungen und Fehlerbehebungen:

- **Einbindung des aktuellen Prüfprotokolls** (Verification Interpreter) 3.10.1: Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtige Änderung:
 - OSCI-PlugIn: Es kann folgendes Verhalten realisiert werden: Enthält die Datei oscicontentdata ein Element <osci:CipherCertificateOtherAuthor>, dann wird der CN des Zertifikats aus dem Element <osci:CipherCertificateOriginator> im Prüfprotokoll nicht als Absender angezeigt, sondern der CN aus dem Zertifikat <osci:CipherCertificateOtherAuthor>. Sollten mehrere <osci:CipherCertificateOtherAuthor> vorhanden sein, wird das Zertifikat, welches als erstes gefunden wird, angezeigt. Alle anderen CN werden dann im Prüfprotokoll als „weitere Absender“ angezeigt.

- **Änderung der Funktion "Weiterleiten":** Derzeit wird beim Weiterleiten einer Nachricht eine neue Nachricht generiert, der Teile der Originalnachricht angehängt werden (Anlagen, Metadaten wie der Nachrichtentyp, Betreffe mit dem Vorsatz "WG:"), andere Bestandteile wie das Prüfprotokoll aber nicht. Zukünftig wird die empfangene Originalnachricht (inkl. aller Bestandteile) als Anlage (zip) zu einer neuen Nachricht beigefügt und weitergeleitet. Der Name der Anlage entspricht der Nachrichten-ID, bspw. "WG_Nachrichten-ID.zip. Für die Nachricht werden aus der Originalnachricht die Angaben zum Nachrichtentyp, der Betreff sowie ggf. die Aktenzeichen übernommen.
- **Aktualisierung von verwendeten Drittbibliotheken:** Es wurden die Bibliotheken Bouncy Castle 1.60 sowie die aktuelle OSCI-Bibliothek 1.8.1 eingebunden. Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Justiz Edition Nutzungsbedingungen" entnehmen.
- **Behebung einer möglichen Schwachstelle in der Kommunikation zum SAFE-Verzeichnisdienst (Signature Wrapping).**
- **Anzeige des Absenders in der Eingangsbestätigung:** Der Name des Absenders (laut Visitenkarte) wird nun wieder angezeigt.

14 Version 3.7.2.1

Bereitstellung: 03.07.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.2.0_HF1
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.12.0
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.10.0
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.0
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.59

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.2.0 auf Version 3.7.2.1 ist **möglich**.

Es muss ein MSI-Installer ab Version 2.0.1 verwendet werden.

	<p>Nutzung des aktuellen MSI-Installers Version 2.0.2:</p> <p>Für die <u>produktive</u> Umgebung steht ein neuer MSI-Installer Version 2.0.2 bereit. Ab dieser Version werden die Anwendungsressourcen abgesichert über https vom Downloadserver der Governikus KG heruntergeladen.</p> <p>Bitte beachten Sie, dass ältere MSI-Installerversionen als die Version 2.0.2 nur bis zum 2. November 2018 verwendet werden können. Stellen Sie daher rechtzeitig auf die neue Version um.</p>
---	--

Verbesserungen und Fehlerbehebungen:

- **Einbindung des aktuellen Prüfprotokolls** (Verification Interpreter) 3.10.0: Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtigen Änderungen:
 - Der VI verwendet seit dieser Version den SOG-IS Plus-Katalog. In dieser Version wurde das Algorithmenkatalog-Schema so erweitert, dass für geeignete Algorithmen, die im SOG-IS-Katalog kein Ablaufdatum erhalten haben, im Prüfprotokoll auch "ohne Ablaufdatum" angezeigt werden kann. Dieses führt zu veränderten Anzeigen in den menschenlesbaren Prüfprotokollen und im XML-Prüfprotokoll. Hier gibt es eine nicht abwärtskompatible Schemaänderung.
 - Das Fehlerhandling bei PDFs mit mehreren Signaturen in einer Revision wurde so verbessert, dass nun immer die Fehlermeldung "Die Signatur konnte nicht verarbeitet werden" angezeigt wird.

- Fehlerbehebung im Zusammenhang mit einer möglichen Schwachstelle bei der Zertifikatsprüfung.

Informationen zum Governikus-Prüfprotokoll finden Sie im Dokument "Anwenderhandbuch Governikus-Prüfprotokoll".

- **Verbesserung im Umgang mit HTML-Dateien (Prüfung auf ausführbaren Schadcode):** Nach dem Empfang von OSCINachrichten in der Anwendung werden einige Nachrichtenbestandteile in HTML-Dateien umgewandelt, um die Anzeige der Daten in der Anwendungsoberfläche zu ermöglichen (Visitenkarte, Nachricht, Eingangsbestätigung, Prüfprotokoll (Nachrichtentyp/OSCI-Betreff)). Die HTML-Dateien werden vor der Anzeige auf enthaltenen Schadcode geprüft und ggf. gefiltert.
- **Verbesserung im Umgang mit externen Zip-Dateien (Verhindern der sog. Zip-Slip-Attacke):** Bei der "Zip-Slip"- Attacke wird versucht, externen Code ins Dateisystem einzuschleusen, indem vorhandene Dateien/Programme überschrieben werden. Der Governikus Communicator bietet eine Funktion zum Importieren von Postfächern an. Bei diesem Vorgang werden zip-Dateien importiert, die zukünftig auf diese Attacke hin überprüft werden.
- **Meldung "Postfach löschen" verbessert:** Der Meldungstext, der dem Nutzer vor dem Löschen eines Postfachs angezeigt wird, wurde optisch verbessert, um dem Nutzer deutlicher zu machen, dass nach dem Bestätigen der Meldung das Postfach wirklich gelöscht wird.
- **Verbesserung im Umgang mit Sonderzeichen in Dateianhängen:** Für die Namen der Dateianhänge sind nur bestimmte Sonderzeichen zugelassen, die verwendet werden. Damit es beim Empfang von Nachrichten, die ggf. nicht zugelassene Sonderzeichen in den Dateinamen enthalten, nicht zu Problemen kommt, werden die Dateinamen bereits beim Versand auf nicht zugelassene Zeichen geprüft und diese durch Leerzeichen ersetzt.
- **Mehrfaches Öffnen eines Postfachs führt zu Fehlbedienung:** Es wurde ein Fehler behoben, der dazu führte, dass ein Postfach mehrfach geöffnet werden konnte.
- **Fehler beim Öffnen eines importierten Postfachs:** Es wurde ein Fehler beim Öffnen eines importierten Postfaches behoben.
- **Aktualisierung von verwendeten Drittbibliotheken.** Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Nutzungsbedingungen" entnehmen.
- **Einbindung der aktuellen client_ca_certs.jar Version 65:** Mit dieser Komponente werden die unterstützten Austellerzertifikate hinsichtlich ihres Signaturlevels in der Anwendung erkannt (Anzeige "Q" oder "F" bei der Auswahl des Signaturzertifikates).

15 Version 3.7.2.0

Bereitstellung: 30.04.2018


Basissysteme:

Governikus Communicator Framework:	Version 3.7.1.2
MCard (Kartenansteuerung):	Version 2.2.3
Certificate Interpreter (CI):	Version 1.11.1.12
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.8.1
Transportschicht (http-Transport):	Version 2.4.0.18
OSCI-Bibliothek:	Version 1.8.0
Algorithmenkatalog (Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms V1.1/BNetzA 2017):	Version 2018
Bouncy Castle	Version 1.59

Online-Update über den MSI-Installer:

Ein Online-Update der Version 3.7.1.0 auf Version 3.7.2.0 ist **möglich**.

Es muss ein MSI-Installer ab Version 2.0.1 verwendet werden.

	<p>Bereitstellung eines aktuellen MSI-Installers Version 2.0.2:</p> <p>Für die <u>produktive</u> Umgebung wird ein neuer MSI-Installer Version 2.0.2 bereitgestellt. Ab dieser Version werden die Anwendungsressourcen abgesichert über https vom Downloadserver der Governikus KG heruntergeladen.</p> <p>Bitte beachten Sie, dass ältere MSI-Installerversionen als die Version 2.0.2 nur bis zum 2. November 2018 verwendet werden können. Stellen Sie daher rechtzeitig auf die neue Version um.</p>
---	--

Verbesserungen und Fehlerbehebungen:

- **Einbindung des aktuellen Prüfprotokolls (Verification Interpreter) 3.8.1:** Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtigen Änderungen:
 - Eignungsprüfung von Signaturalgorithmen: Es wurde ein Fehler bei der Kumulierung der Algorithmen Eignung der Inhaltsdatensignatur behoben.

Informationen zum Governikus-Prüfprotokoll finden Sie im Dokument "Anwenderhandbuch Governikus-Prüfprotokoll".
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.2.3:** Diese Version enthält im Vergleich zur Version 2.1.1HF1 folgende Änderungen:
 - Die Chipkartenlesegeräte vom Hersteller Reiner SCT mit dem Handelsnamen
 - CyberJack pinpad Version 3

- CyberJack e-com
- CyberJack e-com PLUS

wurden aus der Liste der unterstützten Chipkartenlesegeräte entfernt, weil der Hersteller keine Treibersoftware und keine Sicherheitsupdates mehr bereitstellt.

- Mit diesem Release werden die Signaturkarten mit dem Handelsnamen D-TRUST Card 3.1 in den Ausprägungen Einzel-, Stapel- und Multisignatur, herausgegeben durch den qualifizierten Vertrauensdiensteanbieter D-TRUST GmbH, auf Basis vom Kartenbetriebssystem CardOS 5 mit 3.072 Bit-Schlüsseln unterstützt.
- Für diese MCard-Version wurden neue Zertifikate für das Code-Signing und den JCE-Provider verwendet.

Informationen zu unterstützten Karten, Lesegeräten und Betriebssystemen finden Sie im Dokument "Unterstützte Kombinationen Leser-Karten-Betriebssysteme".

16 Version 3.7.1.0

Bereitstellung: 16.01.2018

Basissysteme:

Governikus Communicator Framework:	Version 3.7.1.0
MCard (Kartenansteuerung):	Version 2.1.1HF1
Certificate Interpreter (CI):	Version 1.11.1.12
Verification Interpreter (VI) (Prüfprotokoll):	Version 3.8.0
Transportschicht (http-Transport):	Version 2.4.0.14
OSCI-Bibliothek:	Version 1.8.0
Algorithmenkatalog:	Version 2017
Bouncy Castle	Version 1.59

Online-Update über den Installer:

Ein Online-Update der Version 3.7.0.2 auf Version 3.7.1.0 ist **möglich**.

Verbesserungen und Fehlerbehebungen:

- **Einbindung des aktuellen Prüfprotokolls** (Verification Interpreter) 3.8.0: Diese Version enthält im Vergleich zur Vorversion folgende für diese Anwendung wichtigen Änderungen:
 - Mit der Version wird ein Fehler bei der Eignungsprüfung von Signaturalgorithmen behoben: Der Fehler führte dazu, dass das Prüfergebnis bei nicht mehr geeigneten Paddings nicht korrekt kumuliert wurde.
- **Einbindung der aktuellen Kartenansteuerung (MCard) 2.1.1 Hotfix01**
Informationen zu unterstützten Karten, Lesegeräten und Betriebssystemen finden Sie im Dokument "Unterstützte Kombinationen Leser-Karten-Betriebssysteme".
- **Aktualisierung von Bouncy Castle (auf Version 1.59) und weiterer verwendeter Drittbibliotheken.** Eine Auflistung der verwendeten Drittbibliotheken können Sie dem Dokument "Governikus Communicator Nutzungsbedingungen" entnehmen.