Governikus KG

Governikus Communicator

Release-Übersicht

Governikus Communicator Justiz Edition

Governikus Communicator Justiz Edition 3.7.3.2

Inhaltsverzeichnis

1 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.

2 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).

3 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.

Nutzung des aktuellen MSI-Installers Version 2.0.2:

Für die produktive 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.

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.

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.

4 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.

Nutzung des aktuellen MSI-Installers Version 2.0.2:

Für die produktive 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.

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.

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.

.

5 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.

	**Nutzung des aktuellen MSI-Installers Version 2.0.2:** Für die produktive 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. 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.

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.

6 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.

Nutzung des aktuellen MSI-Installers Version 2.0.2:

Für die produktive 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.

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.

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 OSCI-Nachrichten 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).

7 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.

Bereitstellung eines aktuellen MSI-Installers Version 2.0.2:

Für die produktive 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.

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.

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".

8 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.