



Leitfaden zum Verifizieren signierter Dokumente

Gesetzliche Vorgabe

Gemäß §2 (1) des "Gesetzes zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) sind Behörden vom 01.07.2014 an verpflichtet, "[...] auch einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifiziert elektronischen Signatur versehen sind, zu eröffnen". Daraus ergibt sich die Anforderung an die Behörden, qualifiziert signierte Dokumente, die beispielsweise als Anhang von E-Mails übermittelt werden, zu empfangen, zu prüfen, zu bearbeiten und aufzubewahren. Bitte lesen Sie dazu auch den Abschnitt "Unterstützte Trustcenter" am Ende dieses Leitfadens.

Mit dem Governikus Signer können elektronisch signierte Dokumente verifiziert werden.

Verifizieren von signierten Dokumenten

Benutzen Sie zum Verifizieren von signierten Dokumenten den Governikus Signer in der Basic oder Professional Edition. Mit der Funktion "Verifizieren" des Governikus Signer können Sie die elektronische Signatur prüfen.

Verifizieren von signierten E-Mails

Neben der Prüfung signierter Dokumente ist ebenfalls die Prüfung signierter E-Mails durch den Governikus Signer möglich. Die Signatur von E-Mails wird von den meisten modernen E-Mail-Clients unterstützt, wobei der sogenannte S/MIME-Standard (Secure/Multipurpose Internet Mail Extensions) verwendet wird. Der Governikus Signer kann standardkonforme E-Mail-Signaturen ab S/MIME-Version 3.1 prüfen. Um eine signierte E-Mail prüfen zu können, müssen Sie diese zuerst speichern. Der Governikus Signer unterstützt Sie bei der Verifikation von signierten E-Mails, die als Dateien mit den Endungen `.eml` oder `.msg` gespeichert wurden.

- `.eml`: Das E-Mail-Dateiformat `eml` wird beim Speichern von vielen Mail-Clients benutzt, wie beispielsweise Microsoft Outlook Express, Lotus Notes, Windows Mail oder Mozilla Thunderbird.
- `.msg`: Das E-Mail-Dateiformat `.msg` ist ein eigenes Dateiformat der Microsoft Corporation. E-Mails, die aus dem Mail-Client Microsoft Outlook gespeichert werden, haben die Dateiendung `.msg`. Der Governikus Signer unterstützt die Verifikation für E-Mail-Dateien der Versionen Outlook 2007, Outlook 2010 und Outlook 2013. E-Mails aus älteren Outlook-Versionen müssen vor einer Prüfung in das `.eml`-Format konvertiert werden.


Technischer Hinweis

Wenn Sie eine E-Mail verifizieren, wird dabei nur die E-Mail-Signatur selbst verifiziert. Enthält die E-Mail signierte Dokumente im Anhang, müssen diese signierten Dokumente zuerst gespeichert und dann gesondert verifiziert werden. Signierte Dokumente können nicht zusammen mit der signierten E-Mail verifiziert werden.

Vorgehen - Verifikation signierter Dokumente bzw. E-Mails

Um die Signatur eines Dokuments oder einer signierten E-Mail zu prüfen, gehen Sie wie folgt vor:

- **Speichern der Dokumente bzw. E-Mail:** Markieren Sie die E-Mail in Ihrem E-Mail-Client und speichern Sie die E-Mail mit der Dateiendung `.msg` bei E-Mails in MS Outlook oder mit der Dateiendung `.eml` bei E-Mails in anderen Mail-Clients. Signierte Dokumente müssen ebenfalls vor der Prüfung abgespeichert werden.
- **Aufruf der Verifikationsfunktion:** Starten Sie den Governikus Signer und rufen Sie die Funktion "Verifizieren" auf. Laden Sie eine oder mehrere Dateien in die Dateiauswahl.

	Hinweis: Damit Sie auch die Dateien mit der Endung <code>.msg</code> im Auswahldialog sehen können, geben Sie im Dialog "Dateien auswählen" einen Stern * in der Eingabezeile "Dateiname" ein. Bestätigen Sie die Eingabe mit der "Enter"-Taste. So werden alle Dateien im Verzeichnis angezeigt und können ausgewählt werden.
---	---

- **Dialogseite Optionen:** Im Schritt "Optionen" können Sie bestimmen, ob die Verifikation online erfolgen soll. Dies ist empfohlen, um eine Aussage über die Identität des Signierenden zu erhalten. Bei qualifizierten elektronischen Signaturen ist diese Einstellung zwingend vorgeschrieben. Wählen Sie ein Verzeichnis, in dem das Prüfprotokoll der Verifikation abgelegt wird.
- **Dialogseite Verifizieren:** Klicken Sie auf den Schalter "Verifizieren", um die Verifikation zu starten.
- **Prüfverfahren:** Das Prüfverfahren verifiziert die Integrität und die Identität des Signierenden:
 - **Integritätsprüfung:** Der Governikus Signer führt mit dem Signaturprüf Schlüssel, der im Signaturzertifikat enthalten ist, eine mathematische Signaturprüfung der Daten durch. So wird die Integrität des Dokuments oder der E-Mail geprüft. Mit einem positiven Ergebnis wird bestätigt, dass das signierte Dokument bzw. die signierte E-Mail seit der Signaturerstellung nicht verändert wurde. Bei einer qualifizierten elektronischen Signatur wird zusätzlich noch ermittelt, ob der verwendete Signaturalgorithmus den Anforderungen des Signaturgesetzes genügt.
 - **Überprüfung der Identität des Signierenden:** Nach der erfolgreichen Integritätsprüfung prüft der Governikus Signer das zur Signatur gehörende Signaturzertifikat gegen das Trustcenter (Zertifizierungsdiensteanbieter). Dafür ist eine Online-Verbindung zum Governikus OCSP/CRL-Relay erforderlich. Die Verbindung zum Governikus OCSP/CRL-Relay wird im Dialog "Einstellungen" konfiguriert. Mit Hilfe des Governikus OCSP/CRL-Relays wird geprüft:
 - ob das Trustcenter das Signaturzertifikat, dass die Identität des Signierenden bestätigen soll, tatsächlich vom Trustcenter ausgestellt wurde und ob das Trustcenter vertrauenswürdig ist,
 - ob die Signatur des Dokuments bzw. der E-Mail innerhalb des Gültigkeitszeitraums des Signaturzertifikats angebracht wurde,
 - ob die Signatur des Zertifikats durch das Trustcenter gültig ist und
 - ob das Signaturzertifikat gültig ist oder ob es gesperrt wurde.
- **Prüfergebnis:** Alle oben angegebenen Prüfungen werden als Einzelprüfungen bezeichnet und ergeben zusammen das Gesamtprüfergebnis. Für jedes verifizierte Dokument bzw. E-Mail wird ein Prüfprotokoll erstellt, das im Zielverzeichnis abgelegt

wird. Je nach Konfiguration im Dialog "Einstellungen" kann das Prüfprotokoll als HTML- oder als PDF-Datei erstellt werden.

Das Prüfprotokoll

Das Ergebnis der Verifikation ist im Prüfprotokoll nachzulesen. Für einen schnellen Überblick über das Verifikationsergebnis wird im Governikus Signer nach der Verifikation ein farbiges Symbol vor jede Zeile gestellt, die ein Prüfprotokoll enthält. Die Symbole haben die folgende Bedeutung:

- **Grünes Symbol mit weißem Haken:** Alle durchgeführten Einzelprüfungen haben ein positives Ergebnis. Die Signatur ist gültig.
- **Gelbes Symbol mit schwarzem Ausrufezeichen:** Mindestens eine der Einzelprüfungen ist fehlgeschlagen.



Achtung: Dies bedeutet nicht zwangsläufig, dass die Integrität oder die Authentizität des signierten Dokuments bzw. der signierten E-Mail nicht gegeben ist.

- Gründe für dieses Prüfergebnis, Beispiele: Es ist möglich, dass zum Zeitpunkt der Verifikation ein Trustcenter online nicht erreichbar war. In diesem Fall ist die Empfehlung, die Verifikation zu einem späteren Zeitpunkt erneut durchzuführen. Werden Zertifikate mit dem Signaturniveau "fortgeschritten" geprüft und ist die ausgebende Zertifizierungsstelle nicht im OCSP/CRL-Relay hinterlegt, führt dies auch zu einer gelben Markierung im Prüfergebnis. Das Prüfprotokoll listet alle Gründe für das Prüfergebnis auf.
- **Rotes Symbol mit schwarzem Kreuz:** Mindestens eine der Einzelprüfungen war abschließend nicht erfolgreich. Damit ist entweder die Unverfälschtheit der Inhaltsdaten (Integrität der Daten) nicht sichergestellt oder es konnte die signierende Person abschließend nicht sicher identifiziert werden. Die Signatur ist ungültig.

Unterstützte Trustcenter

Ob das zu einer Signatur gehörende Signaturzertifikat online geprüft werden kann, hängt von der Konfiguration des Governikus OCSP/CRL-Relays ab, dessen Adresse im Governikus Signer im Dialog "Einstellungen" hinterlegt ist. Zur Prüfung der Zertifikate einer Signatur sind im Governikus OCSP/CRL-Relay Verbindungsinformationen und CA-Zertifikate von Trustcentern (Zertifizierungsdiensteanbieter) hinterlegt. Im Rahmen des Projektes Pflege Governikus sind über die Standardkonfiguration des Governikus OCSP/CRL-Relays folgende Zertifizierungsdiensteanbieter (ZDA) konfiguriert:

- alle Zertifizierungsstellen (Trustcenter, Zertifizierungsdiensteanbieter) aus Deutschland, die qualifizierte Signaturzertifikate für offene Nutzergruppen herausgeben,
- alle Zertifizierungsstellen, die fortgeschrittene Zertifikate, Authentisierungs- und/oder Verschlüsselungszertifikate herausgeben, soweit sich diese auf qualifizierten Signaturkarten deutscher Zertifizierungsdiensteanbieter befinden, die qualifizierte Signaturkarten für offene Nutzergruppen herausgeben,
- ausgewählte Zertifizierungsstellen unter der deutschen PKI-1-Verwaltung und
- ausgewählte Bundesländer-PKIs.

Bitte beachten Sie, dass die Konfiguration und Aktualisierung des Governikus OCSP/CRL-Relays in der Verantwortung des Betreibers liegt und daher keine generellen Aussagen über die Konfiguration getroffen werden können.