

Sperrliste der interkantonalen Geldspielaufsicht (Gespa)

Spezifikationen für Fernmeldedienstanbieterinnen (Version 2)

1. Zugriff

1.1. Webserver

Die Publikation der Sperrlisten der interkantonalen Geldspielaufsicht erfolgt auf einer eigenständigen, einfachen Web-Applikation. Diese listet den Inhalt eines Dateiverzeichnisses auf dem Webserver mit dem NGINX autoindex Module (http://nginx.org/en/docs/http/ngx_http_autoindex_module.html) auf.

- URL: <https://blocklist.gespa.ch>
- Verschlüsselung: Domain-validiertes SSL Zertifikat von Lets Encrypt
- Encoding: UTF-8
- Ausgabeformate:
 - HTML: http://lxr.nginx.org/source/src/http/modules/ngx_http_autoindex_module.c#0434
`curl -i -H "Accept: text/html" https://blocklist.gespa.ch`
 - JSON: http://lxr.nginx.org/source/src/http/modules/ngx_http_autoindex_module.c#0698
`curl -i -H "Accept: application/json" https://blocklist.gespa.ch`

1.2. Dateien

Für jede publizierte Sperrliste werden die folgenden Dateien auf dem Webserver abgelegt:

- https://blocklist.gespa.ch/gespa_blocklist_YYYYMMDD.txt
Sperrliste mit allen zu sperrenden Domain-Namen
- https://blocklist.gespa.ch/gespa_blocklist_YYYYMMDD.txt.sign
Signaturdatei zur Verifikation der Datenintegrität der Sperrliste
- https://blocklist.gespa.ch/gespa_blocklist_YYYYMMDD.diff
Liste der Differenz gegenüber der Vorversion
- https://blocklist.gespa.ch/gespa_blocklist_YYYYMMDD.diff.sign
Signaturdatei zur Verifikation der Datenintegrität der Differenzliste

Zudem befinden sich in diesem Verzeichnis auch die notwendigen Dateien zur Verifikation der Datenintegrität:

- `https://blocklist.gespa.ch/blocklist.gespa.ch.pub`
Öffentlicher Schlüssel (Public Key)
- `https://blocklist.gespa.ch/intermediate.pem`
QuoVadis Swiss Regulated CA G3
- `https://blocklist.gespa.ch/ca.pem`
QuoVadis Root CA1 G3

1.3. Direktzugriff aktuelle Sperrliste

Damit der direkte Zugriff auf die aktuellste Version der Sperrliste vereinfacht wird, stehen fixe URLs mit Umleitungen (HTTP 301 Redirect) auf die entsprechenden Dateien zur Verfügung.

- `https://blocklist.gespa.ch/gespa_blocklist.txt`
Umleitung auf die neuste Version der Sperrliste
 - `https://blocklist.gespa.ch/gespa_blocklist.txt.sign`
Umleitung auf die neuste Version der Signaturdatei der Sperrliste
 - `https://blocklist.gespa.ch/gespa_blocklist.diff`
Umleitung auf die neuste Version der Differenzdatei
 - `https://blocklist.gespa.ch/gespa_blocklist.diff.sign`
Umleitung auf die neuste Version der Signaturdatei der Differenzdatei
-

2. Formate

2.1. Sperrliste

- Dateiname: `gespa_blocklist_YYYYMMDD.txt`
(YYYYMMDD entspricht dem Publikationsdatum)
- Encoding: ASCII
- Zeilenumbrüche: Unix \n

Jede Zeile enthält entweder einen Domain-Namen oder eine Kommentarzeile für Metadaten.

Domain-Namen:

- Internationalisierter Domain-Name (IDN): Punycode für Domains mit Sonderzeichen
(https://de.wikipedia.org/wiki/Internationalisierter_Domainname)
- `domain.tld` sperrt auch alle Subdomains `x.domain.tld`, `y.domain.tld`

Metadaten:

- Startzeichen Raute (#)
- #Version: N
Version der Sperrlisten-Spezifikation
- #Serial: YYYYMMDD
Publikationsdatum der Sperrliste

2.2. Differenzdatei

- Dateiname: gespa_blocklist_YYYYMMDD.diff
(YYYYMMDD entspricht dem Publikationsdatum)
- Encoding: ASCII
- Zeilenumbrüche: Unix \n

Die Ausgabe der Differenzdatei gegenüber der Vorgängerversion erfolgt durch die Ausgabe von `git diff`, im Format Unified (https://en.wikipedia.org/wiki/Diff#Unified_format) ohne Kontext (`unified=0`). Sie dokumentiert neue und entfernte Domain-Namen.

2.3. Signaturen

- Dateinamen: gespa_blocklist_YYYYMMDD.txt.sign /
gespa_blocklist_YYYYMMDD.diff.sign
- Encoding: Base64
- Zertifikat: Geregeltes Firmen-Siegel von QuoVadis, geregelt gemäss ZertES (SR 943.03) / VZertES (SR 943.032)
- Hashalgorithmus: SHA-256

3. Kontakt

Bei Fragen betreffend die Umsetzung der Zugangssperre stehen wir Ihnen gerne zur Verfügung (blocklist@gespa.ch).