KULTURSERVER

THE COMMUNITY FOR ART AND CULTURE

Appendix

Technische Details zur Absicherung des Videoangebotes im Kulturserver Netzwerk

Berlin, September 2020

Stiftung kulturserver.de gGmbH

Geschäftsführung: Wolfgang Knauff
Amtsgericht Aachen HRB 10515

USt.-IdNr.: DE 230868040
Steuernr.: 127/602/52603

Mail: redaktion@kulturserver.de

Geschäftsstelle Berlin
Almstadtstraße 4
10119 Berlin
Tel.: +49 30 22667748
Fax: +49 241 33636

www.kulturserver.de

Geschäftsstelle Aachen
Lothringerstraße 23
52062 Aachen
Tel.: +49 241 33686
Fax: +49 241 33636

Im folgenden möchten wir weitere Detailinformationen zur Umsetzung der Absicherung des Videoangebotes im Kulturserver Netzwerk geben.

Das Problem besteht in der Grundeigenschaft aller Internetbasierten Dienste, die durch eine Verlinkung/URL beschrieben werden und damit zunächst mehr oder weniger frei und unmittelbar erreichbar sind. Doch nicht immer ist ein Zugriff erwünscht – wie beispielsweise bei privaten Daten oder bei kostenpflichtigen Videos. Wie genau der Schutz vor ungewolltem Zugriff aussieht soll im Folgenden genauer erklärt werden.

Allgemeine Beschreibung

Kulturserver nutzt Infrastruktur, die in Deutschland lokalisiert ist. Die Server sind vollständig unter der Administration unserer Mitarbeiter*innen und es müssen keine weiteren externen Services/Drittanbieter genutzt werden. Dadurch hat Kulturserver die Sicherheitsangaben direkt im Blick und kümmert sich um die stetige Weiterentwicklung dieser Server.
Die Lagerung und Auslieferung der Videos ist über ein serverseitiges SecureLink Modul gesichert. Ähnlich eine DRM handelt es sich um ein Schlüssel-Schloss-Prinzip, indem ein je Auslieferung spezifischer, ein Mal gültiger Link generiert wird, der dann dir Übertragung der Daten freigibt.
Dies geschieht pro Datensatz, pro Nutzer und zur Laufzeit – d.h. mit zeitlicher Begrenzung. So kann nicht einfach der Link aus dem Code extrahiert und andersartig verwendet werden – oder durch bloße Änderung einer Video ID für andere Videos unberechtigt weiter verwendet werden.

Technische Detailinformationen

Zur Absicherung der Videoangebotes kommt der NginX Secure Modul zu Einsatz (http://nginx.org/en/docs/http/ngx_http_secure_link_module.html).

Es wird verwendet, um die Authentizität angeforderter Links zu überprüfen, Ressourcen vor unbefugtem Zugriff zu schützen und die Gültigkeitsdauer der Links zu begrenzen.

Die Gültigkeit eines angeforderten Links wird überprüft, indem die übergebene Prüfsummen mit dem für die Anforderung berechneten Wert verglichen wird. Wenn ein Link eine begrenzte Lebensdauer hat und die Zeit abgelaufen ist, gilt der Link als veraltet. Der Dienst wird in der Variable $ secure_link verfügbar gemacht.

Ein SecureLink besteht aus vier Komponenten:

Dienst
https://u.culturebase.org
Pfad
z.B. /o/p/e/r/a/operation_k_i_alt_und_neu.2020.film.lang_de.mp4
Gültigkeit
ein GET-Parameter mit Unix-Zeitstempel, z.B. t=1600170000 für eine Gültigkeit bis zum 15.9.2020 13:40
Signatur
ein GET-Parameter zur Absicherung der anderen beiden Werte, z.B. sig=YDvO5x-6EmdAwO1MNIEiJA, Beschreibung siehe unten

Der gesamte Link in diesem Beispiel lautet:
https://u.culturebase.org/o/p/e/r/a/operation_k_i_alt_und_neu.2020.film.lang_de.mp4?t=1600170000&sig=YDvO5x-6EmdAwO1MNIEiJA

Der Streaming-Server kann die Gültigkeit dieses Links ohne weitere Kenntnis von Benutzerkonto oder Session prüfen:

- fehlen die angehängten GET-Parameter ist der Link ungültig
- liegt der Zeitstempel in der Vergangenheit, ist der Link veraltet, also ungültig

Damit ein Benutzer den Zeitstempel nicht einfach selbst anpasst, ist die Signatur nötig. Diese berechnet Film7 aus dem Pfad, dem Zeitstempel und einem geheimen Schlüsselwort, den sowohl Film7, als auch der Streaming-Server kennen:

- passt die Signatur nicht zu den übrigen Informationen, ist der Link ungültig

Ohne die Kenntnis des geheimen Schlüssels kann ein Benutzer keine gültige Signatur berechnen, wenn der Link verändert wird.

Als Signaturverfahren wird einfach eine MD5-Summe über die drei Werte (Pfad, Zeitstempel, Schlüssel) gebildet. Der Singnaturwert ist die Base64-Darstellung dieser MD5-Summe.