

SwiftServe CDN Content Access Control

Feature Note

Confidential

Version 1.0
30/07/2012

Contents

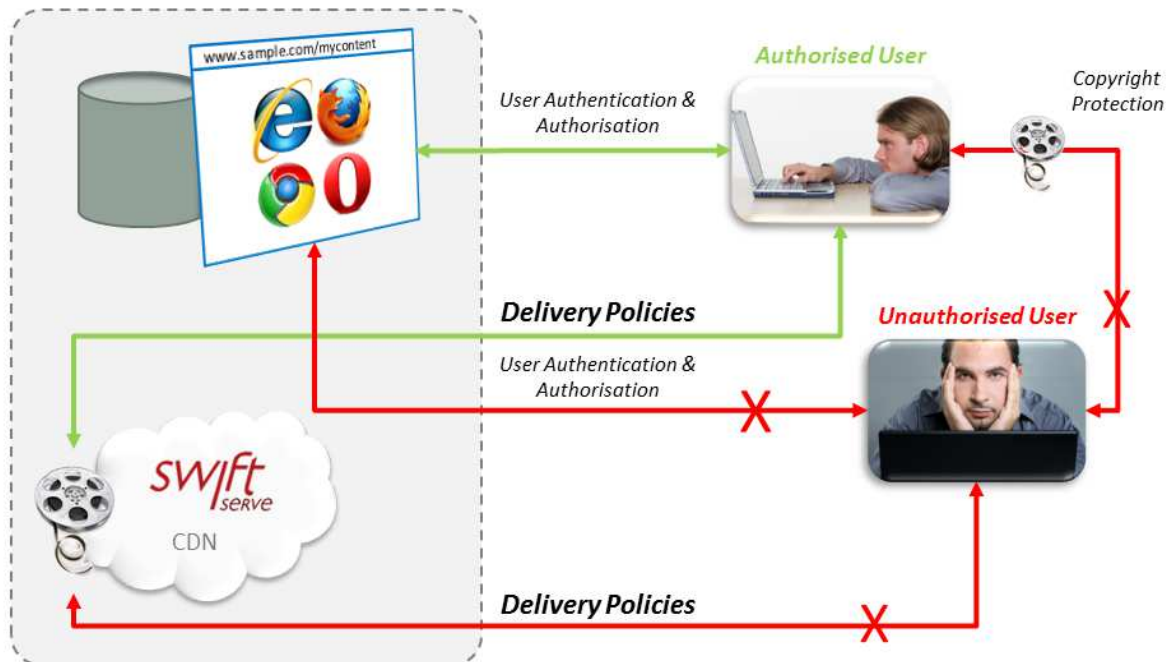
1	Access Control to Content	3
2	SwiftServe CDN Policies	4
2.1	IP-Based Restrictions.....	4
2.2	Geographic (geoIP) Restrictions.....	4
2.3	Token Authentication	4
3	Conclusion.....	5

1 Access Control to Content

Typically content publishers will wish to restrict user-access to the content they are offering, e.g. to protect their revenue and to comply with the rights they have for that content. For example, a content publisher with the rights to the live-streaming of an international sporting event in a specific country will want to make sure only users who have paid the subscription fee and are physically located in that country can watch the event.

Controlling access to content can happen at 3 complementary levels:

- > **User Authentication and Authorisation:** This process determines whether a user is authorised to have access to the content or not. This is the main authentication process, and takes into account factors that are specific to the content publisher's business model, including what services the user has paid for. For that reason, it is typically handled through the content publisher's portal.
- > **Delivery policies:** Once a user has been authenticated, they may request access to content, such as files, videos or live-streams, which are stored and handled by the CDN. SwiftServe CDN uses policies to determine whether the content requested by a user should be delivered to them or not.
- > **Copyright protection:** The content publisher will want to ensure that once a user has downloaded content, e.g. a video or some software, they cannot use it for unauthorised purposes, such as illegal distribution. This is handled by Digital Rights Management (DRM) within the content.



The user authentication and authorisation, and copyright protection are outside the scope of this document. The following sections describe how the SwiftServe CDN ensures the delivery of content to authorised users only.

2 SwiftServe CDN Policies

Policies apply to requests for access to content within the SwiftServe CDN. These requests are in the form of a URL (Uniform Resource Locator, as used for web addresses), for example as a result of the user clicking on a link in the content publisher's portal or when they press "play" on an embedded video. These URLs, which can be static (i.e. pre-stored) or generated on-the-fly by the portal, refer to a location within the SwiftServe CDN.

The policies are created and maintained by the administrator of the content, and are stored in the SwiftServe CDN.

SwiftServe provides 3 types of policies to restrict access to content:

- > IP-based
- > Geographic
- > Token-based authentication

These three methods can be used individually or deployed in any combination, depending on requirements.

2.1 IP-Based Restrictions

The SwiftServe CDN can check that the user requesting the content is doing so from a device with a recognised IP address. Access can be granted or denied to individual IP addresses or to ranges of addresses. For example, this method might be used to restrict access to customers of a particular network service provider or to students on a specific university campus.

2.2 Geographic (geoIP) Restrictions

The SwiftServe CDN can check that the user requesting the content is located in an approved country. It does so using the IP address of the user's device to determine the current location of the user. This method would typically be used to enforce the geographic rights restrictions for particular content.

2.3 Token Authentication

The SwiftServe CDN offers a way to ensure that the URL providing access to content is only valid for authorised users. Effectively, this is a method to secure the URL itself, making it usable for a defined period of time and optionally from a specific IP address only. As a result, this provides an additional level of protection against unauthorised access to content.

This method secures the URL with the help of "tokens" which encrypt the information in the request (i.e. a part of the URL) using a key known only to the content publisher (or network service provider) and SwiftServe. If the encrypted token, which is itself passed with the request (URL) in the form of a string of characters, is missing or not consistent with the information in the request, the content will not be delivered.

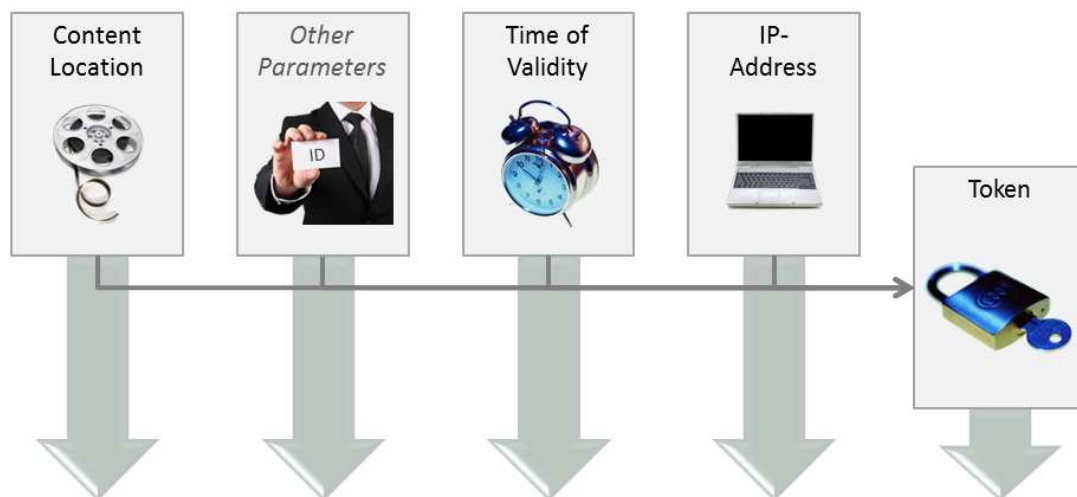
The tokens are generated based on the URL by the content publisher (or network service provider) using tools provided by SwiftServe. The SwiftServe CDN applies the exact same algorithm when it receives the URL, and compares the result with the token supplied in the URL. The tokens can be pre-generated and stored ahead of actual use, or can be generated on the fly based on parameters known only at the time of access by the user (see below).

The tokens have a life-span (start and end time of validity), which is also passed in the URL. The life-span parameters are checked by the SwiftServe CDN to make sure the token is indeed valid at that point in time. The parameters also used to generate the actual token, so any unauthorised changes

to these parameters (e.g. to try and extend the validity of the token) would result in the token being invalid (the encrypted value would no longer match the URL contents).

It is also possible to pass (optionally) the IP address of the authorised device within the URL. The SwiftServe CDN will check that actually device requesting the content has indeed that IP address, before delivering the content. As the IP address passed in the URL is also used to generate the encrypted token, any attempt to change that information will likewise invalidate the token.

In addition, any other parameters can be passed in the URL, e.g. a unique client id or a product id. Though these parameters would not be checked by the SwiftServe CDN, they would be used as part of the encryption so would contribute to securing the URL.



www.sample.com/content?otherparams=xyz&time=201112010601006&etime=20111201100100&ip=1.2.3.4&encoded=1ef46a2b90bec055da32

In short, before serving-up content, the SwiftServe CDN will check that:

- > The token is being used within the authorised time window
- > The IP address of the requesting device is the same as the one supplied in the URL (optional)
- > The token provided is a correct encryption of the relevant part of the URL

If any of those checks fail, the content will not be delivered.

3 Conclusion

The SwiftServe CDN provides a layer of access control which, combined with the user authentication and authorisation provided by the content publisher's portal and the copyright protection provided by DRM, ensures that only authorised users may access content stored in the network.