#### Gancho Tenev

```
employer:
```

Apple Inc

ats committer known for:

cachekey plugin, s3\_auth\_v4, debugging + fixing

contact:

gancho@apache.org

# Access Control Plugin

Apache Traffic Server plugin to enforce access control to the content of the CDN caches

# Why?

- Make sure users are authorized to access the content in CDN caches
- Don't care about the details of third-party authentication and authorization solutions!



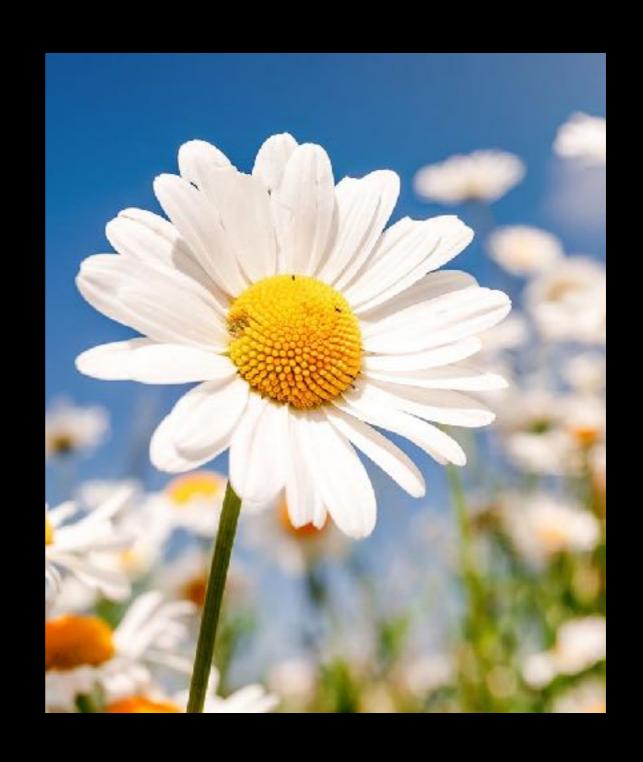
# Enforce only access control at the Edge

- Enforce only access control at the Edge based on access tokens from the Application (Origin)
- Leave the Authentication and Authorization to the Application. They know better!



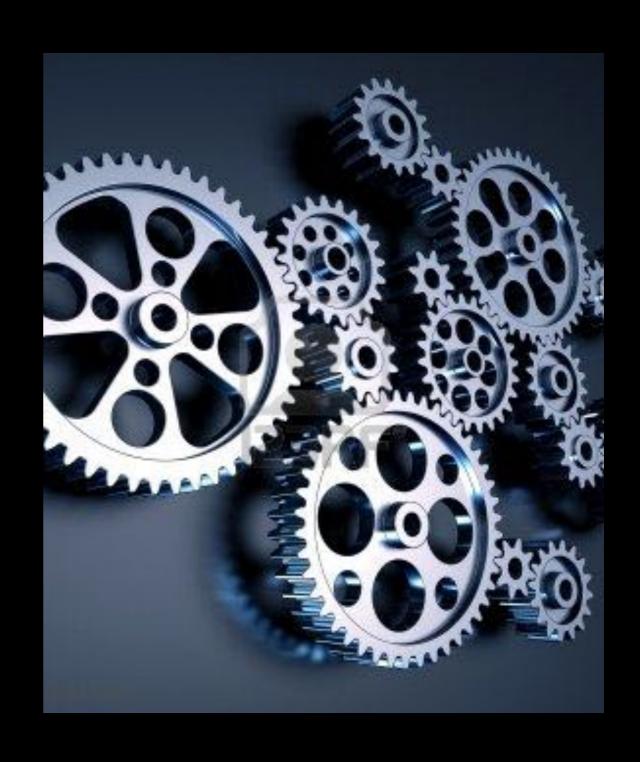
#### Non-intrusive

- The flow works with any Authentication and Authorization mechanisms, supports App-to-App-Authorization.
- Access control is enforced only based on information exchanged between CDN and the Application (Origin)



#### How it works?

- CDN forwards unauthorized requests to Origin and receives an access token in the response
- CDN stores the access token in a cookie in the UA and then uses it to enforce access control to its cache for all following requests.



# Target Audiences

- The Application decides on a set of target audiences around which the access control is enforced, i.e. managers and individual contributors
- The access token contains the target audience id which is an opaque string to CDN
- Based on the target audience CDN could serve different versions of the same documents



## Security

- The flow is blessed by information security experts
- TLS only
- Access token signature types: HMAC-SHA-256, HMAC-SHA-512, RSA-PSS (still not implemented)
- Set-Cookie attributes: HttpOnly, Secure
- Access token and cookie expiration mandatory



#### Future?

- This plugin is still experimental, based on its usage we would likely support more authorization flows.
- There are some common functional areas with URI signing and authproxy plugins, may be at some point it would make sense to reconsider and refactor or consolidate the functionality



### More info?

- Documentation: https:// docs.trafficserver.apache.org/en/latest/ admin-guide/plugins/ access\_control.en.html
- Source code: <a href="https://github.com/apache/trafficserver/tree/master/plugins/">https://github.com/apache/trafficserver/tree/master/plugins/</a>
   experimental/prefetch
- Contact: gancho@apache.org

