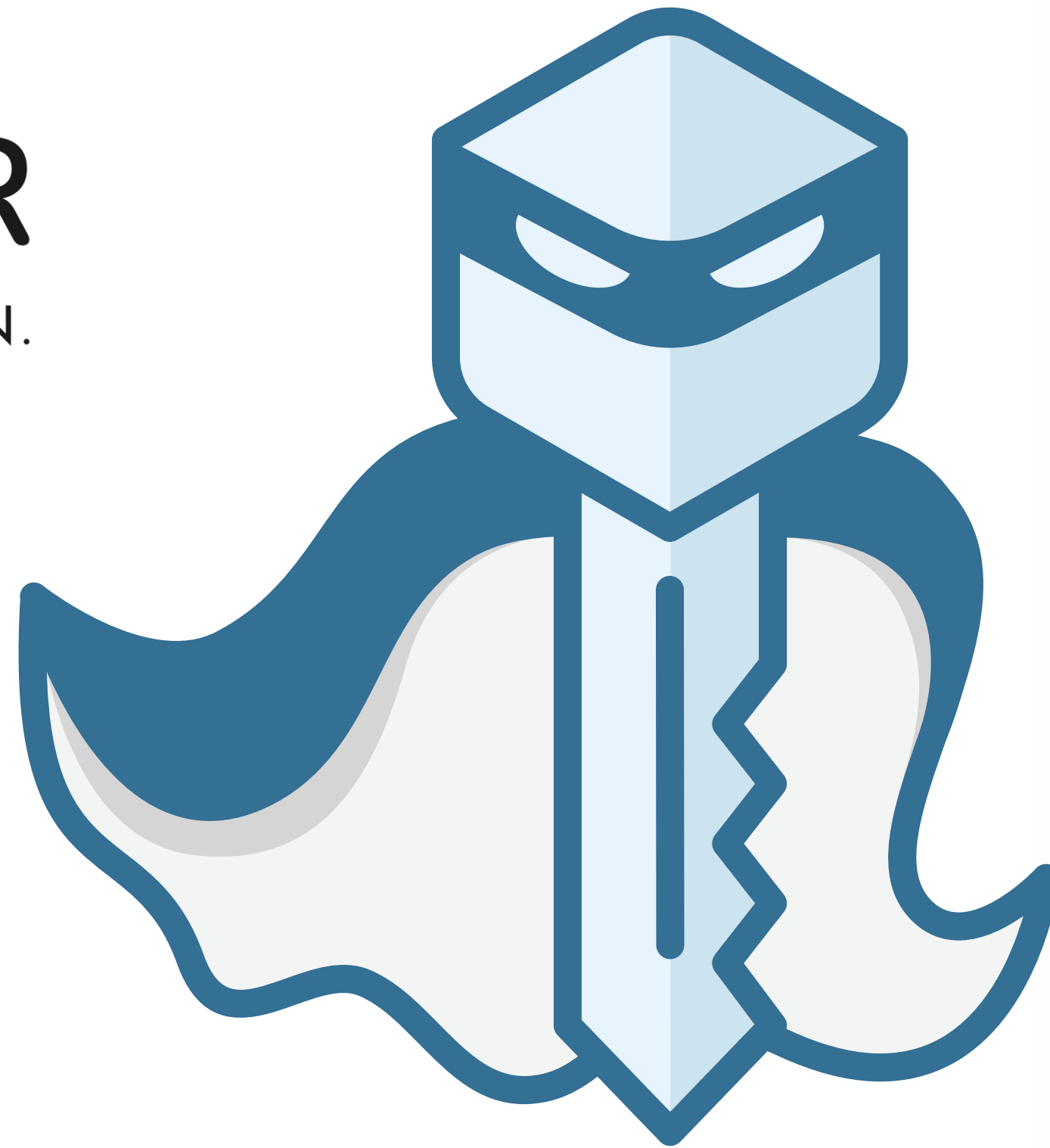




NIKO KÖBLER

CONSULT. DEVELOP. TRAIN.



TOKEN HYGIENE

THE **KEYCLOAK MISTAKES** THAT **90%** OF ALL DEVELOPERS/ADMINS GET WRONG

ABOUT ME

- ▶ Independent Consultant/Architect
- ▶ Doing stuff with & without Computer
- ▶ "Mr. KEYCLOAK" since 2015 (v1.x)
- ▶ Organizer of KEYCLOAK DevDay C
- ▶ Member of various IAM Expert gro
- ▶ Co-Lead of JUG DA (www.jug-da.de)
- ▶ Web: www.n-k.de / Social: @dasniko
- ▶ YouTube: youtube.com/@dasniko
- ▶ Road Cyclist 



KEYCLOAK DevDay 2027

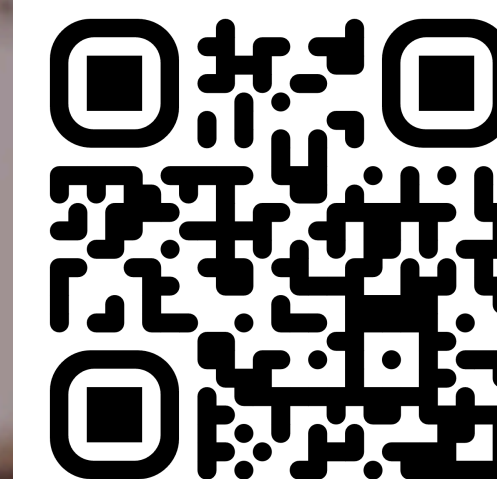
📅 April 8 & 9, 2027 📍 Darmstadt, Germany

The world's largest KEYCLOAK community conference

>>> [Call for Papers](#) <<<

[Subscribe to our newsletter to stay updated!](#)

<https://keycloak-day.dev>



2(!)
Days

200+
Attendees

20+
Talks + Keynote

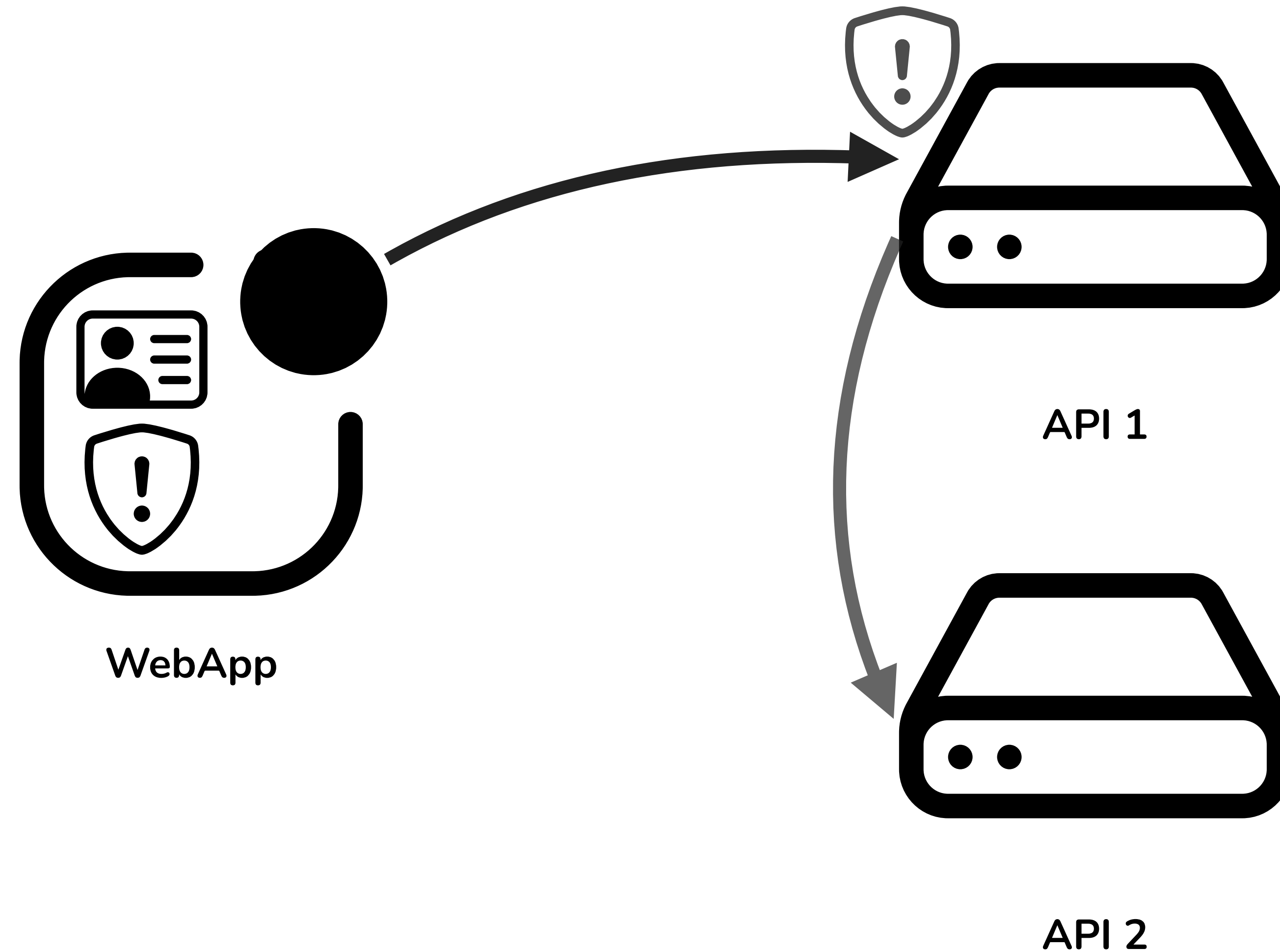
20+
Speakers + Maintainers

TOKEN HYGIENE

DATA MINIMIZATION (GDPR/PRIVACY)

MINIMUM SCOPED TOKENS

SCENARIO: TOKEN PROPAGATION



RFC 9068 - JSON WEB TOKEN (JWT) PROFILE FOR OAUTH 2.0 ACCESS TOKENS

Chapter 6: Privacy Considerations:

The client **MUST NOT** inspect the content of the access token: the authorization server and the resource server might decide to change the token format at any time. ...

The OAuth 2.0 framework assumes that access tokens are treated as opaque by clients.

Administrators of authorization servers should also take into account that the content of an access token is visible to the client. ...

In every scenario, the content of the JWT access token will eventually be accessible to the resource server. It's important to evaluate whether the resource server gained the proper entitlement to have access to any content received in the form of claims, for example, through user consent in some form, policies and agreements with the organization running the authorization servers, and so on.

<https://www.rfc-editor.org/info/rfc9068/>

RFC 9068 - JSON WEB TOKEN (JWT) PROFILE FOR OAUTH 2.0 ACCESS TOKENS

Chapter 4: Validating JWT Access Tokens:

Resource servers receiving a JWT access token **MUST** validate it in the following manner.

- ▶ ...
- ▶ The resource server **MUST** validate that the "aud" claim contains a resource indicator value corresponding to an identifier the resource server expects for itself. The JWT access token **MUST** be rejected if "aud" does not contain a resource indicator of the current resource server as a valid audience.
- ▶ ...

<https://www.rfc-editor.org/info/rfc9068/>

RFC 8693: OAUTH 2.0 TOKEN EXCHANGE

Why Token Exchange matters:

- ▶ No "God"-tokens, 1 token = 1 purpose
- ▶ No replay in all directions *(if client X can call resource Y and resource Z, it's also possible vice-versa)*
- ▶ Don't expose/leak internals into the client *(client needs to know all of the resource servers)*
- ▶ Keep "Least Privilege" approach *(only roles and scopes of one resource server are in the token)*
- ▶ Enforce proper authorization rules *(only client X is allowed to access resource Y)*

As an illustration:

"Multi-Audience" is a master key that you give to the guest - one that also opens the data center - in the hope that the guest won't find his way there. "Token Exchange" means: The guest has a key for the front desk, and only the receptionist can retrieve a one-time key for the data center using their own ID and the guest's authorization.

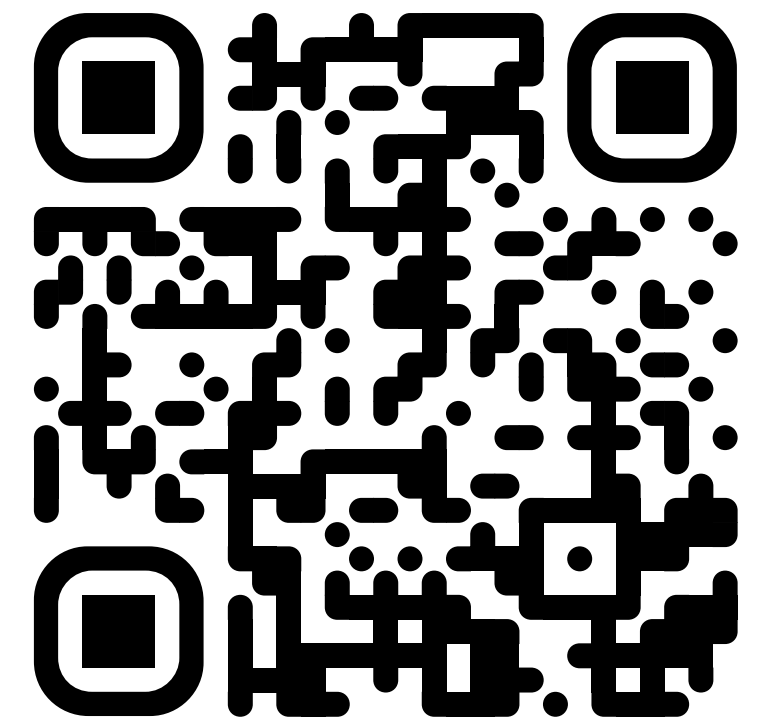
<https://www.rfc-editor.org/info/rfc8693/>



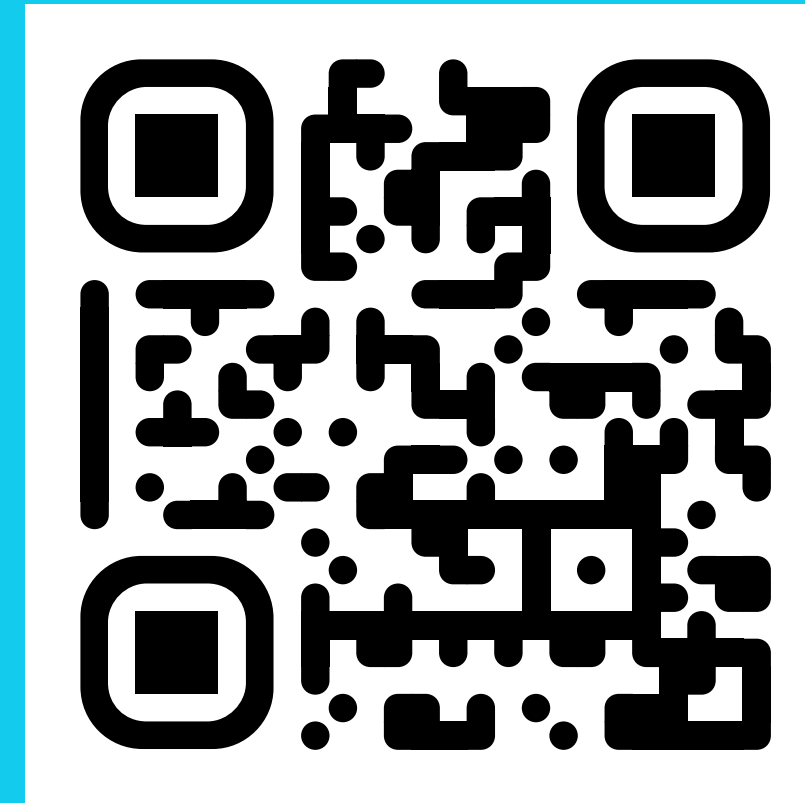
The Keycloak-Token-Configuration Mistake, 90% of All Developers Do (and How To Avoid It)

Niko Köbler IT-Beratung

<https://www.youtube.com/watch?v=iuu8NdqAFcw>



THANK YOU.
ANY QUESTIONS?



More info / slides: <https://linktr.ee/dasniko>



NIKO KÖBLER | www.n-k.de | niko@n-k.de | [@dasniko](https://twitter.com/dasniko)

MY PUBLIC RESOURCES AND STUFF

- ➔ Overview / Links: linktr.ee/dasniko
- ➔ Website / Info: www.n-k.de
- ➔ YouTube / Videos: youtube.com/@dasniko
- ➔ GitHub / Examples: github.com/dasniko
- ➔ Speakerdeck /Slides: speakerdeck.com/dasniko

