Eén gebruiker, één token: waarom dat – soms – een béter idee kan zijn

Tijdens een recent project voor een SAAS-platform dat verenigingen en stichtingen ondersteunt, stuitte ik onder andere op het vraagstuk: hoe beheer je gebruikerssessies op een manier die **veilig**, **overzichtelijk** en **praktisch** is?

De gangbare aanpak

In veel moderne webapplicaties is het de standaard dat een gebruiker meerdere tokens tegelijk kan hebben. Logisch ook: je logt in op je laptop, je telefoon, misschien nog een tablet — en alles blijft netjes actief.

Betrekkelijk 'nieuw' in deze materie, volgde ik aanvankelijk ook dat pad. Tot ik tijdens de eerste tests zag wat er gebeurde: tokens begonnen zich op te stapelen. Oude, ongebruikte, verlopen — maar soms nog steeds geldige — tokens bleven in de database hangen. En dat zette me aan het denken.

Wat als we het anders doen?

Want hoe handig het ook klinkt, meerdere tokens per gebruiker brengen ook risico's met zich mee. Niet alleen qua performance — hoe meer tokens, hoe meer er bij elke verificatie doorzocht moet worden — maar vooral qua veiligheid. Een token dat ooit is aangemaakt, maar nooit is opgeruimd, kan in theorie nog steeds misbruikt worden. Zeker in een omgeving waar meerdere gebruikers, soms met meerdere rollen en lidmaatschappen, tegelijk actief zijn. Dan wil je niet dat er ergens een 'vergeten' token rondslingert dat toegang geeft tot gevoelige gegevens.

Mijn keuze: één gebruiker, één token

Daarom koos ik voor een model waarbij elke gebruiker op elk moment maar één geldig token heeft. Bij elke actie — inloggen, gegevens ophalen, iets opslaan — wordt het token ververst. Het oude vervalt direct. Klinkt misschien streng, maar het levert wel wat op:

- ***Performance***: minder tokens in de database betekent snellere verificatie.
- ***Security***: een token dat net is aangemaakt, is minder kwetsbaar dan eentje die al weken 'meezeilt'.
- ***Overzicht***: geen dubbele sessies, geen verwarring, geen 'losse eindjes'.

Maar werkt het ook?

Goede vraag. Want eerlijk is eerlijk: de specifieke oplossing en implementatie ervan — die ik in dit project heb gekozen — heeft zich nog niet in een grootschalige praktijkomgeving bewezen.

Het is vooralsnog een theoretisch model, gebaseerd op eerdere ervaringen, logische redenering en het anticiperen op mogelijke risico's.

Toch geloof ik dat het zinvol is om al in de ontwerpfase keuzes te maken die performance en veiligheid structureel **kunnen** bevorderen. Liever een doordacht fundament dat zich later ook nog eens bewijst, dan een 'standaard' model dat achteraf moet worden bijgesteld.

Tot slot

Het concept ‘één gebruiker, één token’ *an sich* zal niet nieuw zijn. Sterker, ga er zelfs vanuit dat anderen hier al eerder mee geëxperimenteerd hebben. Zou dan ook graag **die** ervaringen horen. Wellicht kunnen we **elkaar** dan helpen bij het nóg robuuster maken van deze oplossing.

“Soms is juist het bewust afwijken van de standaard de sleutel tot een betere oplossing …“

Reageren op dit stukje? Mail naar info@foxserv.nl o.v.v. 'Reactie op Eén gebruiker, één token'