

Technisch paspoort WCAG Radar

Browserextensie voor Chrome, Edge en Firefox. Voor informatiebeveiligers die de extensie beoordelen voordat hun organisatie hem toestaat.

Versie van dit document	21 oktober 2026
Beschreven versie	WCAG Radar 2.46. De bron staat op 2.46.17.
Uitgever	Proper Access B.V., Keizersgracht 520 H, Amsterdam. KVK 95350985
Contact	info@properaccess.nl , 085-505 58 90

In het kort

- De extensie doet niets tot de gebruiker op de knop in de werkbalk klikt. Dan draait hij alleen in dat ene tabblad.
- Alle checks draaien lokaal in de browser. Geen enkele bevinding en geen enkel stuk van de geteste pagina gaat naar Proper Access of naar een andere partij.
- Zonder licentie verstuurt de extensie niets. Met licentie gaat er ongeveer één keer per dag één verzoek naar onze eigen server, met alleen de licentiesleutel erin.
- Rechten: activeTab, scripting en storage, plus toegang tot twee eigen domeinen. Geen toegang tot alle websites, geen geschiedenis, geen cookies, geen netwerkverkeer onderscheppen.
- Alle code zit in het pakket. De extensie laadt geen code van buiten, is niet geobfusceerd en bevat geen bibliotheken van derden.
- Onze server staat bij Hetzner in Helsinki. Er zit geen Amerikaanse partij in de keten van de extensie.

Wat de extensie doet

WCAG Radar laat toegankelijkheidsproblemen zien op de pagina die de gebruiker open heeft. Een redacteur, ontwerper of ontwikkelaar zet per onderwerp een check aan, en de Radar markeert de elementen op de pagina die aandacht nodig hebben. Hij werkt ook op pagina's achter een inlog, op intranetten en op localhost, omdat hij in de browser van de gebruiker rekent en onze server die pagina's nooit ziet.

Een deel van de checks is gratis. Een ander deel en de knop Rapport opslaan vragen een licentie. Welke checks wat zijn, staat op testtoegankelijkheid.nl/wcag-radar.

Identificatie in de winkels

Gebruik deze id's voor een allowlist of een geforceerde installatie via het browserbeleid van je organisatie.

Extensie-id per browser

Browser	Id	Winkel
Chrome	ppnojdoamdffcokjapadjkcggbdnfamc	Chrome Web Store
Edge	ofmanijiiffoehlpbegbdnchonjjdpfb	Edge Add-ons
Firefox	wcag-radar@properaccess.nl	Firefox Add-ons, vanaf Firefox 140

Er is geen versie voor Safari. De winkels lopen soms een paar patchversies achter op de bron, omdat elke winkel een release eerst beoordeelt. Op 21 oktober 2026 stond in Firefox Add-ons 2.46.12 en in Edge Add-ons 2.46.14. De versie in de Chrome Web Store is niet zonder inloggen op te vragen en hebben we voor dit document niet gecontroleerd.

Rechten

Het manifest is Manifest V3. Dit zijn alle rechten die de extensie vraagt.

Rechten in het manifest

Recht	Waarvoor	Wanneer gebruikt
activeTab	Tijdelijke toegang tot het tabblad waarin de gebruiker op de knop klikt.	Alleen na een klik, alleen in dat tabblad. De toegang vervalt als de gebruiker naar een andere pagina gaat.
scripting	Het paneel en de checks in dat tabblad zetten.	Na een klik op de knop.
storage	De licentiesleutel en het licentiebewijs lokaal bewaren.	Alleen als de gebruiker een sleutel invoert. Zonder licentie staat er niets in.
https://testtoegankelijkheid.nl/* https://wcagtoolkit.com/*	De licentiesleutel inwisselen voor een ondertekend bewijs. Beide domeinen zijn van Proper Access en draaien op dezelfde server.	Ongeveer één keer per dag, alleen met een ingevoerde sleutel.

Wat er niet in het manifest staat

- Geen `<all_urls>` en geen host-rechten op andere domeinen dan de twee hierboven.
- Geen `content_scripts`: er draait niets vanzelf op pagina's die de gebruiker bezoekt.
- Geen `tabs`, `history`, `cookies`, `webRequest`, `declarativeNetRequest`, `downloads`, `clipboardRead` of `nativeMessaging`.

Een geautomatiseerde test controleert dat de rechten in het gebouwde pakket exact deze lijst zijn. Die test draait voor elke release; komt er een recht bij, dan faalt hij en gaat de release niet naar de winkel.

In Firefox verklaart de extensie `data_collection_permissions` met `required: ["none"]` en `optional: ["authenticationInfo"]`. Firefox vraagt de gebruiker dus apart om toestemming voordat de licentiesleutel voor het eerst verstuurd wordt. In de Chrome Web Store staat bij Privacy practices de categorie Authentication information aangevinkt, om dezelfde reden.

Hoe de extensie draait

- **Achtergrondscript.** Een service worker in Chrome en Edge, een event page in Firefox. Hij reageert op twee dingen: een klik op de knop, en een verzoek van het paneel om de optiepagina te openen.
- **Het paneel.** Na de klik zet het achtergrondscript `lens.js` uit het pakket in het tabblad. Dat script draait in de isolated world van de extensie: het deelt de DOM met de pagina, maar niet de JavaScript-omgeving. Het paneel zelf staat in een shadow root op de pagina.
- **Lezen, niet veranderen.** De checks lezen de DOM en de berekende stijlen. Om elementen te markeren zet de Radar eigen markeringen op de pagina, die weer weg zijn als je de check uitzet of het paneel sluit.
- **Beschermdde pagina's.** Op `chrome://`- en `about:`-pagina's, in de winkels en in de PDF-viewer laat de browser geen enkele extensie toe. Daar doet de knop niets.
- **Escaping.** Tekst van de pagina die in het paneel komt, gaat door de eigen functie `PA.esc()`. De overige toewijzingen aan `innerHTML` bevatten vaste teksten uit de extensie zelf.

Netwerkverkeer

Dit is al het verkeer dat de extensie kan veroorzaken. Alleen de eerste regel gaat vanzelf; de rest begint met een handeling van de gebruiker.

Verzoeken van de extensie

Verzoek	Bestemming	Wat gaat er mee	Wanneer
Licentie controleren	POST /api/licentie/token op <code>testtoegankelijkheid.nl</code> of <code>wcagtoolkit.com</code>	Alleen de licentiesleutel. Geen gegevens over de geteste pagina, geen cookies.	Ongeveer één keer per dag, en alleen als er een sleutel is ingevoerd. Na een mislukte poging een uur niet. Tijdslimiet 5 seconden.
Animatie in afbeeldingen	De servers waar de afbeeldingen op de geteste pagina al vandaan komen	Een gewoon verzoek om die afbeelding, zoals de browser dat ook doet. De Radar leest hooguit de eerste 256 KB om te zien of het bestand beweegt.	Alleen als de gebruiker de check Automatische beweging aanzet.

Verzoek	Bestemming	Wat gaat er mee	Wanneer
Reflow-weergave	Dezelfde pagina die getest wordt	Een gewoon paginaverzoek, met de sessie van de gebruiker, in een gesandboxt kader van 320 pixels breed. Lukt dat niet, dan een venster van 320 pixels breed.	Alleen als de gebruiker de check Reflow aanzet.
Links in het paneel	wcagtoolkit.com, testtoegankelijkheid.nl, www.properaccess.nl en ishetb1.nl	Gewone links naar achtergrondartikelen.	Alleen als de gebruiker op de link klikt.
Vraag aan expert	testtoegankelijkheid.nl/vragen of wcagtoolkit.com/questions	In de link: de naam van de check, het thema, de rol, de versie van de Radar, en het domein plus pad van de geteste pagina. De queryreeks en het anker van die pagina worden eraf gehaald, omdat daar sessie-id's en herstelltokens in kunnen staan.	Alleen als de gebruiker op de link klikt.

Goed om te weten voor een intranet: bij Vraag aan expert staat het pad van de interne pagina in de link, bijvoorbeeld `https://intranet.example.nl/hr/verlof`. Wil je dat niet, dan is het advies aan gebruikers die link niet te gebruiken. Er is geen instelling om hem uit te zetten.

Wat er niet gebeurt

- Geen telemetrie, geen analytics en geen foutrapportage vanuit de extensie.
- Geen code ophalen. Alles wat draait zit in het pakket uit de winkel.
- Geen verbinding met een taalmodel of een andere dienst van derden.

De bookmarkletversie van de Radar werkt anders: die haalt het script bij elke start op bij ons, en wij tellen per dag hoe vaak dat gebeurt, per taal. Dit document gaat over de extensie.

Gegevens en opslag

In de browser van de gebruiker

Wat de extensie lokaal bewaart

Gegeven	Waar	Toelichting
Licentiesleutel	<code>storage.local</code> van de extensie	Alleen als de gebruiker een sleutel invoert. Onversleuteld, zoals alles in de opslag van een extensie. Weg bij het verwijderen van de extensie, of met de knop op de optiepagina.
Licentiebewijs	<code>storage.local</code>	Ondertekend bewijs met een licentie-id, het id van de ondertekensleutel, het niveau en de looptijd. Geen naam, geen e-mailadres.

Gegeven	Waar	Toelichting
Status van de licentie	<code>storage.local</code>	Wanneer het bewijs is opgehaald, wanneer een poging mislukte, en de reden als de server de sleutel weigert.
Bevindingen	Alleen in het geheugen van het tabblad	Weg als het tabblad sluit of herlaadt. De extensie schrijft niets in <code>localStorage</code> of cookies van de geteste site.
Rapport	De downloadmap van de gebruiker	Alleen als de gebruiker op Rapport opslaan klikt. Het HTML-bestand wordt in de browser gemaakt en bevat de bevindingen, met per bevinding een verwijzing naar het element en de tekst erin. Het gaat niet via onze server.

Het rapport kan tekst van de geteste pagina bevatten. Valt die pagina onder een rubricering, dan valt het rapport daar ook onder.

Op onze server

- Van een licentiesleutel bewaren we alleen een SHA-256-hash. De sleutel zelf staat alleen bij de gebruiker.
- Per licentie tellen we hoeveel bewijzen er per dag zijn afgegeven. Dat is één getal per dag, zonder IP-adres en zonder browsergegevens. Er wordt nooit automatisch op geblokkeerd.
- Weigeringen tellen we per dag per reden, zonder sleutel en zonder account.
- De remmen op het verzoek, 20 per uur per sleutel en 300 per uur per IP-adres, slaan de sleutel en het IP-adres op als gepeperde hash.
- De webserver schrijft geen toegangslag. Het IP-adres bereikt de server wel, zoals bij elk verzoek, maar het wordt niet weggeschreven.

De licentie

- **De sleutel.** Een willekeurige reeks van 24 bytes met het voorvoegsel `ta_`. Elke medewerker krijgt een eigen sleutel, die we los kunnen intrekken.
- **Het bewijs.** De server ondertekent het met Ed25519 en het geldt zeven dagen. De extensie controleert de handtekening met de Web Crypto API tegen publieke sleutels die in het pakket zitten. Een bewijs dat niet klopt, wordt geweigerd, ook als het van ons eigen adres komt.
- **Offline en storingen.** Ligt onze server eruit of blokkeert het netwerk onze domeinen, dan blijft de licentie werken tot het bewijs verloopt. Daarna valt de extensie terug op de gratis checks. Het paneel wacht hooguit 2 seconden op de server en opent dan met wat er lokaal bekend is.
- **Intrekken.** Een ingetrokken sleutel krijgt geen nieuw bewijs meer. Omdat een bewijs zeven dagen geldt, kan het tot zeven dagen duren voordat de betaalde checks bij die gebruiker dichtgaan.
- **Sleutelrotatie.** De extensie kent een lijst publieke sleutels en het bewijs zegt welke het ondertekende. Zo kunnen we de ondertekensleutel vervangen zonder dat licenties stoppen. De privésleutel is op de server zelf gemaakt en heeft die machine niet verlaten.
- **Grenzen.** De code staat leesbaar bij de gebruiker. Wie hem aanpast, kan de betaalde checks openzetten. Dat is een kwestie van licentievoorwaarden en raakt de veiligheid van jouw omgeving

niet.

Server en hosting

De server achter de licentiecontrole

Hosting	Eigen server bij Hetzner Online GmbH, een Duits bedrijf. Datacenter hel1-dc2 in Helsinki, Finland. Back-ups op een Hetzner Storage Box.
TLS	Caddy op de eigen server. Er zit geen CDN of reverse proxy van een derde tussen.
Headers	HSTS met includeSubDomains, Content Security Policy, X-Content-Type-Options, Referrer-Policy en Permissions-Policy. Een test haalt elke publieke pagina door Chromium met precies dit beleid.
Database	PostgreSQL in een container zonder open poort naar het internet. Alleen de applicatie praat ermee.
Antwoord van het endpoint	Cache-Control: no-store. CORS staat open voor elke herkomst, omdat de herkomst van een extensie per installatie verschilt. Er gaan geen cookies mee, en het antwoord hangt alleen af van de sleutel in het verzoek.
Verwerkers	Voor de extensie geen. De andere diensten van de website, zoals e-mail en betalingen, staan op testtoegankelijkheid.nl/privacy .

Code, build en updates

- **Geen code van derden.** Het pakket bevat alleen eigen code: het achtergrondscript, de licentielogica, de optiepagina en `lens.js`. Er zitten geen npm-pakketten in, dus er is geen keten van afhankelijkheden om te beoordelen.
- **Niet geobfusceerd en niet geminificeerd.** `lens.js` is de leesbare bron achter elkaar gezet, met een licentiebanner erboven. Je kunt het pakket uitpakken en de code lezen.
- **Reproduceerbaar.** De build gebruikt alleen de standaardbibliotheek van Node.js en is deterministisch: dezelfde bron geeft byte voor byte hetzelfde pakket. Mozilla krijgt bij elke release de bron en de bouw instructies, en kan het ingediende pakket zelf nabouwen.
- **Beoordeling en ondertekening.** Elke versie gaat door de beoordeling van de winkel. De winkels ondertekenen de pakketten en verspreiden de updates; de browser installeert ze automatisch.
- **Wijzigingen.** Het overzicht per versie staat op testtoegankelijkheid.nl/wcag-radar/changelog. Bij elke versie in de winkel horen release notes in het Nederlands en het Engels.
- **Broncode.** De repository is niet openbaar. De code in het geïnstalleerde pakket is volledig leesbaar.

Beheer in je organisatie

- **Toestaan.** Zet het id uit de tabel Extensie-id per browser op de allowlist van het browserbeleid. Voor een geforceerde installatie gebruik je hetzelfde id.

- **Zonder licentie.** De gratis checks werken zonder enig netwerkverkeer. Je kunt de extensie toestaan en de twee domeinen blokkeren; dan werken alleen de gratis checks.
- **Met licentie.** Het verkeer naar testtoegankelijkheid.nl en wcagtoolkit.com via HTTPS moet dan toegestaan zijn. Gebruikers met een Nederlandstalige browser gebruiken het eerste domein, de andere talen het tweede.
- **Verwijderen.** Bij het verwijderen van de extensie wist de browser de opslag van de extensie, dus ook de sleutel.

Kwetsbaarheden melden

- Contactadres: info@properaccess.nl, ook vermeld in `/.well-known/security.txt` volgens RFC 9116 op beide domeinen.
- Het beleid staat op testtoegankelijkheid.nl/kwetsbaarheid-melden. Binnen 5 werkdagen een inhoudelijke reactie. Openbaarmaking in overleg, met 60 dagen na de melding als uitgangspunt.

Wat we niet hebben

Deze punten zullen in een beoordeling naar voren komen. We noemen ze hier zelf.

- Er is geen onafhankelijke pentest van de extensie. Op 31 augustus 2026 hebben we de webapplicatie op de code nagelopen. De extensie viel buiten die ronde.
- De licentiesleutel staat onversleuteld in de opslag van de extensie. Dat geldt voor elke extensie die iets bewaart; de browser biedt geen versleutelde opslag.
- Een ingetrokken licentie werkt nog tot zeven dagen door.
- De broncoderepository is niet openbaar. De code die bij de gebruiker draait wel.

Heb je een vraag die dit document niet beantwoordt, mail dan naar info@properaccess.nl.