

# **/// Authenticatiebeheerbeleid**

## **1 INTRODUCTIE**

Authenticatie is een begrip waar dagelijks gebruik van wordt gemaakt. Een voorbeeld: een burger wil online een adreswijziging aanvragen, maar hoe kan u als lokaal bestuur met zekerheid weten wie deze aanvraag doet? Authenticatie draait om de vraag: hoe kan met zoveel mogelijk zekerheid worden bepaald dat een individu is wie hij of zij beweert te zijn?

U kan zich wel voorstellen dat het belang om individuen te controleren groter wordt naarmate de gevoeligheid van de informatie of handeling van de persoon of organisatie die zich authenticceert, toeneemt. Lokale besturen werken met gevoelige informatie en daarom is het van belang om een degelijk authenticatiebeheer te hebben. Om een succesvol beleid te implementeren is het ook belangrijk dat het toezicht van dit beleid wordt toegewezen aan een beleidsmedewerker. Deze persoon heeft de verantwoordelijkheid en de bevoegdheid om de toepassing en naleving van het beleid op te volgen en eventuele inbreuken hiervan te rapporteren.

## **2 WET- EN REGELGEVING**

Het is zeer belangrijk om uw authenticatiemethodes af te stemmen op dat wat de methode moet controleren, omdat bepaalde authenticatiemethodes moeten voldoen aan de nationale of Europese regelgeving.

Voor lokale besturen is met name de naleving van de eIDAS-verordening<sup>1</sup> van groot belang. Deze regelgeving stipuleert dat EU-burgers net zo gemakkelijk en veilig zaken moeten kunnen doen met buitenlandse overheidsdiensten als in hun eigen land. Concreet betekent dit dat buitenlandse EU-burgers met hun eigen identiteitskaart moeten kunnen inloggen op Belgische overheidsdiensten, inclusief lokale besturen. Met het oog op deze Europese dienstverlening is het aangewezen om na te gaan welke dienstverleningen binnen uw lokale bestuur wel of niet beschikbaar moeten zijn voor buitenlandse EU-burgers en uw website en betalingssysteem als het nodig is aan te passen (Bancontact is niet beschikbaar in het buitenland).

## **3 BELEID**

### **Organisatorische maatregelen**

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden met betrekking tot authenticatiebeheer. Bij het inrichten van deze processen en procedures is het belangrijk om de informatieklassering in het oog te houden, aangezien dit een bepalende factor is in de keuze voor adequate authenticatiemiddelen. Bijkomend is het belangrijk om de juistheid en continuïteit van deze voorwaarden op te volgen en te rapporteren naar het management.





## 5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
eIDAS	eIDAS staat voor electronic IDentification, Authentication and trust Services en is naast de gekende digitale sleutels een nieuwe aanmeldmethode om uzelf bij andere Europese landen te identificeren.	<a href="https://www.vlaanderen.be/aanmelden-bij-de-overheid-mijn-digitale-sleutels/aanmelden-via-eidas">https://www.vlaanderen.be/aanmelden-bij-de-overheid-mijn-digitale-sleutels/aanmelden-via-eidas</a>
SSO	Met Single Sign On (SSO)-oplossingen kunnen gebruikers dezelfde inloggegevens gebruiken om in te loggen bij vele systemen en toepassingen.	<a href="https://cyberguide.ccb.belgium.be/nl/single-sign-ssu">https://cyberguide.ccb.belgium.be/nl/single-sign-ssu</a>
MFA	Multifactor-authenticatie is een elektronische authenticatiemethode waarbij gebruikers pas toegang krijgen tot een website of applicatie nadat gebruikers zich twee (of meer) keer geauthenticeerd hebben.	<a href="#">Toegangsbeheer   Vlaanderen.be</a>

## REFERENTIES

- Goede praktijken rond identiteit- en toegangsbeheer (CCB): <https://cyberguide.ccb.belgium.be/nl/identiteit-toegangsbeheer>
- Minimale IAM maatregelen Vlaamse Overheid: [Vo Informatieclassificatie - Minimale maatregelen - IAM\\_xle0xg.pdf \(vlaanderen.be\)](#)

////////////////////////////////////