Notitie Forum Standaardisatie

FORUM STANDAARDISATIE

Agendapunt:	Authenticatie		
Bijlagen:	Quality authenticator scheme, STORK		
Aan:	Forum Standaardisatie		
Van:	BFS		
Datum:	25 september 2009	**Versie**	0.3
Betreft:	Indeling van authenticatiemiddelen		

Doel
U wordt gevraagd om:

A. M.b.t. de beoordeling van de veiligheid van authenticatiemiddelen:

1. Onderzoek te laten doen of voor de indeling van authenticatiemiddelen, gebruikt voor het afnemen van diensten in de semi-publieke sector, de STORK QAA indeling als de standaard gebruikt kan worden;
2. Bij geschiktheid de verantwoordelijke beleidsdepartmenten (BZK en EZ) te vragen om deze standaard aan te melden voor de ”pas toe of leg uit” lijst.
3. Bij geschiktheid bestaande authenticatiemiddelen te duiden t.o.v. de vier niveaus van deze standaard.

B. M.b.t. de beoordeling van welk veiligheidsniveau van authenticatie mijn dienst nodig heeft:

4. Onderzoek te laten doen naar een geschikte standaard om de benodigde hoogte van authenticatiemiddel voor een dienst in te schalen.

Toelichting

Ad. 1
Voor het afnemen van diensten van de overheid moet in sommige gevallen authenticatie[1] middelen worden gebruikt zoals DigiD. Er wordt ook binnen het programma eHerkenning gekeken naar het gebruik van markmiddelen om te authenticeren voor diensten inde (semi)publieke sector. De gebruikte authenticatiemiddelen verschillen in de mate van betrouwbaarheid die ze garanderen. In Nederland is er echter geen standaard om authenticatiemiddelen objectief te waarderen op betrouwbaarheid.

In mei 2008 heeft het College het Forum gevraagd om “zo mogelijk aan te geven welk betrouwbaarheidsniveau nodig is voor welk type transactie.” Dit op basis van de adviezen die staan in opdracht van het Forum opgestelde rapport *Verkenning authenticatie* (KPMG, 2007). Hier is geen direct gevolg aangegeven, onder andere doordat er internationaal geen overeenstemming was over welke indeling in niveaus te hanteren. Recentelijk is er echter

[1] Authenticatie: het bewijzen van een geclaimde identiteit (KPMG (2007), *Verkenning authenticatie*, Amstelveen).

in het Europese STORK[2] project een standaard ontwikkeld voor de een indeling in betrouwbaarheidsniveaus van authenticatiemiddelen.

Op basis van een eerder rapport van de IDABC[3] heeft STORK een indeling gemaakt in vier authenticatieniveaus (de QAA levels). Deze indeling wordt omarmt door de 29 participanten, waaronder Nederland (het ministerie van Binnenlandse Zaken speelt een prominente rol binnen het project), Frankrijk en Oostenrijk. De vier niveaus zijn gerelateerd aan de eisen die gesteld worden aan de zekerheid van iemands identiteit. Als er voor een dienst grote zekerheid nodig is dat de persoon die zich aanmeld ook daadwerkelijk is wie hij zegt te zijn, dan is er dus een hoog niveau authenticatie nodig.

Voor de indeling van de niveaus wordt gekeken naar zowel de organisatorische als technische factoren. Bij het organisatorische factoren wordt gekeken naar identificatie procedure, het afgifteproces van identiteitstokens (bijvoorbeeld paswoorden, maar ook pasjes met chips erop), en de kwaliteit van de certificerende autoriteit. Bij de technische aspecten wordt o.a. gekeken naar het type en robuustheid van de identiteitstoken en de kwaliteit van het mechanisme dat gebruikt wordt voor de gebruikersauthenticatie. Elk van deze factoren wordt gescoord, en de zwakst scorende factor bepaalt het niveau van het authenticatiemiddel. Voor meer detail over het raamwerk, zie het bijgevoegde rapport.

Ad. 2
Om adoptie van deze standaard te bevorderen is het raadzaam om de standaard als deze voldoet aan de criteria op de lijst voor “pas toe of leg uit” te laten zetten.

Ad. 3
In het STORK rapport zijn de DigiD niveaus gerelateerd aan de QAA indeling. De Nederlandse overheid heeft volgens het STORK overzicht niet het hoogste (4) en laagste niveau (1) van authenticatie. De DigiD met gebruikersnaam en paswoord (DigiD laag) wordt ingeschaald op niveau 2 van de QAA, DigiD met SMS (DigiD midden) wordt ingeschaald op niveau 3 van de QAA[4]. Er lijkt niet gekeken te zijn naar alternatieve authenticatiemiddelen die ook door de Nederlandse overheid worden gebruikt, zoals de pincode die de Belastingsdienst naast DigiD gebruikt of de alternatieve face to face toevoeging voor het EPD. Om geen discussie te krijgen over hoe veilig een authenticatiemiddelen is, is het raadzaam om de gebruikte middelen te duiden t.o.v. de vier niveaus van deze standaard.

Ad. 4
Het indelen van de authenticatiemiddelen is slechts één kant van wat nodig is om te zorgen voor een goede match van diensten met auhthenticatiemiddelen. Dienstenaanbieders (overheidsorganisaties) moeten ook bepalen wat het beste authenticatie niveau is voor hun diensten. Hiervoor moet een analyse worden gemaakt van de risico’s die gebruikers van de diensten waarbij hun identiteiten worden bepaald lopen. Tevens moet gekeken worden naar het risico dat ontstaan als een dienstverlener ten onrechte de dienst verleent en de maatschappelijke/ economische/ veiligheidsgevolgen daarvan. Het type dreigingen en waarschijnlijkheid en impact van deze dreigingen moeten hierbij worden meegenomen, net

[2] Secure Identitiy Across Border Linked, grote pilot voor interoperabele identiteiten tussen landen. Het gaat hier met name om work package 2, D 2.3, *Quality authenticator scheme*, zie de bijlage en http://www.eid-stork.eu

[3] IDABC (2007), *eID Interoperability for PEGS, proposal for a Multi-level authenctication mechanism and a mapping of existing authentication mechanisms*.

[4] Het niet hebben van het hoogste niveau kan oa betekenen dat Nederlanders niet alle diensten in het buitenland mogen afnemen. STORK raadt dan ook aan om dit niveau wel te ontwikkelen.

als de gevoeligheid en vertrouwelijkheid van de uitgewisselde informatie. Er zijn een aantal richtlijnen en methodes om een dergelijke analyse te maken, maar geen dominante standaard. Verschillende landen hebben eigen standaarden ontwikkeld, afgeleid van internationale standaarden. Nederland heeft niet een standaard manier om zijn processen in te schalen. Dit kan leiden tot de vreemde situatie dat voor dezelfde dienst bij gemeente x een ander authenticatieniveau wordt gebruikt dan bij gemeente y. Erger is als bepaalde diensten een (veel) te laag betrouwbaarheidsniveau hebben, omdat de inschaling niet met een goede methode is gebeurd. Onderzoek is daarom nodig naar wat voor de publieke sector in Nederland een goede standaard is om het benodigde authenticatieniveau mee te bepalen.