Change 424 definitief (SPOED)

Changemanagement Programma van Eisen PKIoverheid

Feb 20, 2020

Oorspronkelijke datum indiening	20 Jan 2020
Extern opgelegd	Ja
Indiener	Mozilla
Auteur voorstel	Jochem van den Berge
Spoed	Ja
Toepassing	

PvE Deel 1: Introductie		PvE deel 3d: Autonome Apparaten	√
PvE deel 2 Algemene eisen aan TSP's		PvE deel 3e: Server	√
PvE Deel 3: Basiseisen		PvE deel 3f: Extended Validation	√
PvE Deel 3: Aanvullende Eisen		PvE deel 3g: Private Services	
PvE deel 3a: Organisatie Persoon	√	PvE deel 3h: Private Server	
PvE deel 3b: Organisatie Services	√	PvE deel 3i: Private Personen	
PvE deel 3c: Burger	√	PvE deel 4: Begrippenlijst	

Bestaande eis (zo ja, welke)	7.1-pkio171, 6.1.1-pkio89
Omschrijving verzoek	In Mozilla Policy 2.7 worden er nieuwe eisen c.q. verduidelijkingen gesteld aan de manier waarop handtekeningen dienen te worden geëncodeerd. Dit naar aanleiding van enkele issues die in 2019 zijn gemeld bij Mozilla. In principe beschrijven deze nieuwe eisen niets nieuws, daar deze voortkomen uit normatieve referenties die ook al in RFC5280 zijn opgenomen. Veiligheidshalve neemt de PA genoemde eisen wel op in het PvE door aanpassing van enkele bestaande eisen. Tevens maakt de PA van deze mogelijkheid gebruik om een scoping issue van eis 6.1.1-pkio89 te corrigeren, de bewoording daarvan aan te passen en de opmerking te verwijderen (daar het hier gaat om de publieke root kan een afwijkend algoritme alleen gekozen worden indien dit bij de browsers wordt toegestaan, dus de genoemde mogelijkheid was een dode letter)
Tekstvoorstel	Aanpassing eis 6.1.1-pkio89. Deze aangepaste eis wordt van toepassing op delen 3a t/m 3d (was onterecht ook nog van toepassing op 3e) Het algoritme en de lengte van de cryptografische sleutels die de TSP gebruikt voor het genereren van de sleutels van certificaathouders moeten voldoen aan de eisen die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 119 312. Daarnaast moet de TSP ook de eisen te volgen die staan beschreven in Hoofdstuk 5.1 en 5.1.1 van de meest actuele Mozilla Root Store Policy. Het gebruik van RSA-PSS MAG wel, maar wordt afgeraden. Aanpassing eis 7.1-pkio171:

	Een TSP MOET zich beperken tot de signature algoritmes zoals gedefineerd in hoofdstuk 5.1 (en subparagrafen) van de Mozilla Root Store Policy. Het gebruik van RSA-PSS MAG wel, maar wordt afgeraden.
Impactanalyse	Bij de PA onbekend. Volgens Mozilla is dit een expliciete omschrijving van hetgeen er al verplicht is via (normatieve) referenties in RFC5280. Desondanks dat adviseert de PA wel aan TSP's om dit goed te controleren met hun CA vendor. De opmerking over ECDSA is feitelijk een voortzetting van het huidige profiel/eis, RSA-PSS wordt in de Mozilla policy nu toegestaan, maar niet in software ondersteunt (vandaar het advies van de PA om dit niet te gebruiken).
Argumentatie	Zie omschrijving.
Uitspraak Wijzigingenoverleg	SPOED
Uitspraak Stelseloverleg	SPOED
Uiterlijke datum effectuering wijziging	1-03-2020