Collis

Forum Standaardisatie
T.a.v. de heer Knubben
Postbus 84011
2508 AA Den Haag

Leiden, 13 september 2010

Betreft: Openbare consultatie expertadvies SHA-2
Geachte heer Knubben,

Bij deze reageer ik op uw brief aangaande openbare consultatie expertadviezen, en dan specifiek op het advies betreffende SHA-2. Hieronder beantwoord ik uw vragen:

1. Bent u het eens met het advies om MD5 te vervangen door SHA-2 op de lijst met gangbare standaarden. [pagina 5 van het expertadvies].
Antwoord: Ja, de risico's die het gebruik van MD5 met zich mee brengt dienen absoluut te worden mitigeert. De vervanging van MD5 door SHA-2 draagt voor de komende decennia bij aan de onweerlegbaarheid van authenticatie- en integriteitscontrolemechanismen.

2. Bent u het eens met het geadviseerde functionele toepassingsgebied van SHA-2? [paragraaf 3.1 van het expertadvies]
Antwoord: Ja, echter omdat het toepassingsgebied authenticatie- en integriteitscontrole zo breed is geformuleerd dient op voorhand coulant te worden gehandeld onder het "leg uit" principe.

Toelichting:
Collis B.V. is betrokken bij de standaardisatie en implementatie van elektronische reis-, identiteit-, registratie-, en autorisatiedocumenten zoals paspoort, identiteitskaart, European Citizen Card (ECC), elektronische rijbewijs, tachograaf, taximeter en standaarden voor bancaire transacties (betalingsverkeer).

Collis B.V. constateert dat er een aantal specifieke (overheids-) applicaties zijn waarin authenticatie- en integriteitscontrolemechanismen gebruikt worden die deel uitmaken van internationaal geaccepteerde of concept standaarden, waarin ook Hash algoritmen worden gebruikt. In de meeste gevallen is er een keuze mogelijk tussen SHA-2 en (een) ander(-e) hash algoritme(-n), maar soms is SHA-2 ook niet in de standaard gedefinieerd.

Een overzicht:

- *ICAO 9303, betreffende Machine Readable Travel Documents (zoals paspoorten)* De standaard definieert het gebruik van SHA-1 hash op enkele punten. Het gebruik van SHA-2 is toegestaan. Voor het lezen van reis- en identiteitdocumenten conform de standaard wordt van applicaties dus verwacht ook SHA-1 te ondersteunen.
- *CEN 15480, betreffende de nog concept standaard voor de Europese Citizen Card* De concept standaard staat naast het gebruik van SHA-2 tevens het gebruik van SHA-1 toe. Voor het

lezen van ECC kaarten conform de standaard wordt van applicaties dus verwacht ook SHA-1 te ondersteunen.

- *ISO18013, betreffende de nog concept standaard voor het Europese rijbewijs* De concept standaard staat naast het gebruik van SHA-2 tevens het gebruik van SHA-1 toe. Het gebruik van SHA-2 wordt aanbevolen (recommended). Voor het lezen van rijbewijsdocumenten conform de concept standaard moet uitgegaan worden van applicaties die ook SHA-1 te ondersteunen.
- *Annex 1B van Council Regulation (EEC) No 3821/85 of 20 December 1985, betreffende standaard voor tachograaf* De annex definieert het gebruik van SHA-1 hash als verplicht. Het gebruik van SHA-2 is nog niet gedefinieerd / vastgelegd in de standaard. Wel wordt er hard gewerkt aan een update van de annex (en standaard).
- *Regeling specificaties en typegoedkeuring boordcomputer taxi, Staatscourant 19 juli 2010* De standaard definieert het gebruik van SHA-1 en SHA-2 hash (keuze). Dit betekent dat SHA-1 ook nog ondersteund moet worden.

Daarnaast wordt in het betalingverkeer vaak gebruik gemaakt van hashing middels SHA-1. Het tempo van overgaan naar de SHA-2 standaard wordt gedreven vanuit de banken en toezichthouders. Indien de overheid betalingsapplicaties verwerft, dient het “leg uit’ principe te worden toegepast.

3. Bent u het eens met de conclusie van de experts ten aanzien van de uitsluitingcriteria? [paragraaf 3.2 van het expertadvies]
Antwoord: Ja

4. Bent u het eens met de conclusie van de experts inzake de openheid van de standaard SHA-2? [paragraaf 3.3 van het expertadvies]
Antwoord: Ja

5. Bent u het eens met de conclusie van de experts dat er in voldoende mate consensus is over het gebruik van SHA-2 in plaats van MD5? [paragraaf 3.4 van het expertadvies]
Antwoord: Ja, mits aan het gestelde onder paragraaf 2 wordt voldaan.

Met vriendelijke groet,
Collis BV