FS-20101011.05D

Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE
Concept COLLEGE NOTITIE

Agendapunt:	05 Lijst open standaarden		
Bijlagen:			
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	November 2010	**Versie**	0.91
Betreft:	Advies over vervanging MD5 door SHA-2 op lijst met gangbare open standaarden		

Waarom is een keuze belangrijk?
MD5 en SHA-2 zijn standaarden voor cryptografische algoritmen die gebruikt worden voor beveiligingsmiddelen, bijvoorbeeld voor het genereren van een elektronische handtekening. De betrouwbaarheid van een beveiligingsmiddel is sterk afhankelijk van de betrouwbaarheid van het gebruikte algoritme. Van MD5 is al enige jaren bekend dat deze zwakheden bevat en deze standaard wordt door veel organisaties (waaronder GOVCERT.NL) afgeraden voor beveiligingsdoeleinden zoals een elektronische handtekening.

Kunt u met een gerust hart "ja"zeggen?
Het voorliggende advies is het resultaat van een expertonderzoek uitgevoerd door een expert van TNO. Het opgestelde expertadvies is publiek geconsulteerd en besproken in het Forum Standaardisatie. Alle in de consultatie ontvangen reacties (10) onderschrijven het expertadvies.

Zijn er risico's verbonden aan de keuze?
Het gebruik van standaarden op de lijst met gangbare standaarden heeft geen verplichtend karakter. Dit betekent dat organisaties niet gedwongen zijn de standaard te gebruiken als dit bepaalde risico's met zich meebrengt. Vervanging van MD5 door SHA-2 zal juist bijdragen aan het verminderen van (beveiligings)risico's.

Doel

Datum
1 oktober 2010

Het College Standaardisatie wordt gevraagd in te stemmen met:

1. de vervanging van MD5 door SHA-2 op de lijst met gangbare standaarden;
2. het volgende functioneel toepassingsgebied: "cryptografische hash-algoritme ten behoeve van authenticatie en integriteitscontrole "

Toelichting

Ad. 1 Vervanging MD5 door SHA-2
MD5 en SHA-2 zijn zogenaamde "cryptografische hash algoritmen" die uit een willekeurige hoeveelheid gegevens (bijvoorbeeld een stuk tekst) een unieke "vingerafdruk" (van een vaste vooraf vastgestelde lengte) kunnen genereren. Een wijziging in de gegevens zal leiden tot een wijziging in de vingerafdruk. De vingerafdruk is uniek in de zin dat:

- het praktisch onmogelijk is om gegeven een vingerafdruk een tekst te maken die na toepassing van het algoritme tot dezelfde vingerafdruk zal leiden. Oftewel: als je over de vingerafdruk beschikt, kun je vaststellen of de achterliggende gegevens authentiek zijn.
- het praktisch onmogelijk is om twee willekeurige gegevenssets (b.v. twee stukken tekst) te vinden die leiden tot dezelfde vingerafdruk.
  Daarnaast is het praktisch onmogelijk om, gegeven een vingerafdruk, de achterliggende gegevens te achterhalen.

Bovenstaande eigenschappen maken dat deze algoritmen bij uitstek geschikt zijn voor het gebruik in bepaalde beveiligingstoepassingen, zoals een elektronische handtekening.

Van MD5 is al enige jaren bekend dat deze een aantal zwakheden bevat waardoor bovenstaande eigenschappen niet meer gegarandeerd kunnen worden. Daarom hebben verschillende organisaties, waaronder GOVCERT, besloten om MD5 niet meer te gebruiken voor beveiligingsdoeleinden.

SHA-2 is oorspronkelijk door de Amerikaanse National Security Agency (NSA) ontworpen en door het Amerikaanse National Institute of Standards and Technology (NIST) gepubliceerd. Tegenwoordig wordt de standaard beheerd door ISO. Het gebruik van SHA-2 wordt veilig geacht tot 2030.

De standaard is door een TNO expert getoetst tegen de vier uitsluitingcriteria:

- eenmalige opname
- betrekking op informatie-uitwisseling
- geen beperkt werkingsgebied
- niet wettelijk verplicht

Vervolgens is de standaard door dezelfde TNO expert getoetst tegen de criteria voor de lijst met gangbare open standaarden: openheid en consensus. Op elk van de zes criteria is positief geadviseerd. Tijdens de publieke consultatieronde zijn hierop 10 reacties ontvangen, die allen instemden met het opgestelde advies.

Ad. 2 Functioneel toepassingsgebied
Het voorgestelde functionele toepassingsgebied is: "*cryptografische hash-algoritme ten behoeve van authenticatie en integriteitscontrole*".

Opgemerkt wordt dat dit toepassingsgebied breder is dan het toepassingsgebied waarmee MD5 nu op de lijst is opgenomen (maar dit wel omvat). Voor standaarden

op de lijst met gangbare open standaarden wordt geen organisatorisch werkingsgebied vastgesteld, omdat de lijst geen verplichtend karakter heeft.

Welk probleem wordt daarmee opgelost?
Het MD5 algoritme bevat zwakheden waardoor het onvoldoende betrouwbaar is voor beveiligingstoepassingen. SHA-2 kent deze zwakheden niet, en wordt veilig geacht tot 2030.

Waar gaat het inhoudelijk over?
MD5 en SHA-2 zijn cryptografische algoritmen die gebruikt worden voor beveiligingsmiddelen, bijvoorbeeld voor het genereren van een elektronische handtekening.

Zijn er alternatieven voor de voorgestelde keuze?
Er bestaan alternatieve cryptografische algoritmen die ook genoemd worden in het expertadvies. Voor al deze algoritmen geldt echter dat deze ófwel weinig gebruikt worden, ófwel onveilig geacht worden.

De expertgroep is dus van mening dat er geen daadwerkelijke concurrerende standaarden zijn op het gekozen toepassingsgebied.

Schets van de expertgroep en de consultatie
Het expertonderzoek is uitgevoerd door een TNO onderzoeker die veel kennis heeft van beveiligingsaspecten en algoritmen. Na het uitvoeren van het onderzoek is een advies opgesteld is dat publiek geconsulteerd is. Tijdens de consultatie zijn 12 reacties ontvangen die alle het advies onderschreven.

In één van de reacties wordt gewezen op een aantal voor de overheid relevante specifieke standaarden en regelingen waarin ook hash-algoritmen worden genoemd. 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. Hieronder volgt het 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.

SHA-2 wordt toegevoegd aan de lijst met gangbare open standaarden en niet aan de "pas toe of leg uit"-lijst. De lijst met gangbare standaarden heeft geen verplichtend karakter, waardoor de opname niet op gespannen voet staat met de genoemde standaarden en regelingen.

Mogelijke consequenties van opname op de lijst met standaarden
Vervanging van MD5 door SHA-2 zal bijdragen aan het verminderen van (beveiligings)risico's bij overheidsorganisaties. Ondanks het niet-verplichtende karakter van de lijst met gangbare standaarden, maakt opname wel expliciet dat niet (meer) voor MD5 gekozen zou moeten worden, maar voor het betere SHA-2 alternatief.

Communicatie
Zowel het Forum Standaardisatie als het Programmabureau Nederland Open in Verbinding zullen aandacht besteden aan de vervanging van MD5 door SHA-2 op de lijst met gangbare open standaarden.