Aanmeldingsformulier

Vragen met een * zijn verplicht.

Persoonsgegevens

Geslacht: [...]
Voornaam *: [...]
Tussenvoegsel(s) *: n.v.t.
Achternaam *: [...]
Organisatie *: Bureau Forum Standaardisatie
Functie *: [...[
Telefoonnummer *: [...]
E-mailadres *: [...]
Welke relatie bestaat er tussen uw organisatie en de aangemelde standaard? *

- Anders: De te verwijderen standaard (MD5) staat op de door College Standaardisatie vastgestelde lijst met gangbare standaarden.

Melding

Wat voor soort melding wilt u doen? *

- Voorstel om een geheel nieuwe standaard aan te melden
- Voorstel om een standaard van een lijst te verwijderen

Een open standaard of een set van open standaarden?

Meldt u één standaard aan of een set van bij elkaar horende standaarden? *

- één standaard

Voorstel om een nieuwe standaard aan te melden

Informatie over de open standaard

Volledige naam *: Secure Hash Algorithm
Afkorting *: SHA-2
Versie *: SHA-2 (Deze kent een aantal varianten met hetzelfde algoritme maar met verschillende hash-lengtes, namelijk SHA-224, SHA-256, SHA-384 en SHA-512)
Toepassingsgebied *: Overlappend met MD5, namelijk cryptografische hash-algoritme t.b.v. authenticatie (bijv. via digitale handtekeningen) en fingerprints (bijv. via checksums).
Beheerorganisatie *: NIST (ontwikkelaar), ISO, ETSI, IETF
Locatie (Website) *:
> NIST / FIPS PUB 180-3: http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf
> ISO/IEC 10118-3: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39876
> ETSI TS 102 176-1: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=25179
> IETF: http://www.ietf.org/rfc/rfc3174.txt (alleen SHA-1)

Bijdragen aan de doelen van de lijsten

In hoeverre neemt de interoperabiliteit toe door voor deze standaard een pas toe of leg uit beleid te hanteren of om de standaard op de lijst met veelgebruikte standaarden te zetten?*
> Door hetzelfde open algoritme te gebruiken kan informatie-uitwisseling met een hoog technisch beveiligingsniveau plaatsvinden.

In hoeverre neemt de leveranciersonafhankelijkheid toe door voor deze standaard een pas toe of leg uit beleid te hanteren of om de standaard op de lijst met veelgebruikte standaarden te zetten? *
> Omdat SHA een open standaard is kan iedere leverancier het algoritme implementeren. Daardoor is de overheid niet afhankelijk van een of een beperkt aantal leveranciers. De recente problematiek rondom de beveiliging van de OV-chipkaart toont het risico van afhankelijkheid van gesloten (proprietary) algoritmes, in dit geval Crypto-1 van NXP Semiconductors (zie: http://www2.ru.nl/media/pressrelease.pdf).

Waaruit blijkt de behoefte voor het gebruik van deze standaard door de verschillende (semi) publieke organisaties? *
> O.a. PKIoverheid en UZI kiezen voor deze standaard.

Toepassingsgebied

Voor welke doeleinden zou de standaard het beste toegepast kunnen worden?
> Cryptografische hash-algoritme t.b.v. authenticatie (bijv. via digitale handtekeningen) en fingerprints (bijv. via checksums).

Voor welke doeleinden wordt de standaard al toegepast? *
> Idem

Indien er al een open standaard voor het beoogde toepassingsgebied is opgenomen op de lijst met open standaarden, is de aangemelde standaard interoperabel met de desbetreffende standaard op de lijst?
> Reeds opgenomen standaard is MD5. Deze is niet interoperabel met SHA.-2

Organisatorisch werkingsgebied

Binnen welke organisaties zou de standaard het beste gebruikt kunnen worden?*
> Overheden en instellingen uit de (semi-) publieke sector

Binnen welke organisaties wordt de standaard al gebruikt?
> Organisaties die PKIoverheid gebruiken (http://www.pkioverheid.nl/), UZI-pas (http://www.uziregister.nl/nieuws/nieuwsbrieven/uzitechniek/)

Wat is de mate waarin de standaard al gebruikt wordt?
- o Niet of nauwelijks gebruikt
- x Enkele organisaties gebruiken de standaard
- o De standaard wordt door de helft van de organisaties gebruikt
- o De meerderheid van de organisaties gebruikt de standaard
- o Bijna elke organisatie gebruikt de standaard

Openheid

De standaard dient kosteloos of tegen nominale kosten beschikbaar te worden gesteld. Waaruit blijkt dat dit voor uw standaard het geval is? *
> De specificatie is bij NIST kosteloos te downloaden.

Het intellectueel eigendomsrecht van de standaard moet vrijelijk beschikbaar zijn (geen royalty). Waaruit blijkt dat dit voor uw standaard het geval is? *
> Zie: http://www.nist.gov/public_affairs/disclaim.htm
> Er staat geen copyright-notice in de specificatie.

Zijn er beperkingen voor hergebruik van de standaard? *
> Voor zover bekend niet.

Hoe worden besluiten genomen in de beheerorganisatie? *
> Zie: http://csrc.nist.gov/groups/ST/index.html

Welke organisaties hebben inspraak in de besluitvorming? *
> Zie: http://csrc.nist.gov/groups/ST/index.html
> Zie: http://csrc.nist.gov/groups/ST/hash/email_list.html
> Zie: http://csrc.nist.gov/groups/ST/hash/index.html

Is het mogelijk om zelf inspraak te krijgen in de ontwikkeling van de standaard?*
> Ja, er is een public competition voor een nieuwe versie van SHA. Zie: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

Bruikbaarheid

Welke standaarden concurreren met uw standaard? *
> Zie: http://en.wikipedia.org/wiki/Cryptographic_hash_function#Cryptographic_hash_algorithms
> SHA-2 concurreert met het oudere SHA-1. Het Amerikaanse beleid mbt SHA staat hier: http://csrc.nist.gov/groups/ST/hash/policy.html

“March 15, 2006: The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. Federal agencies should stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010. After 2010, Federal agencies may use SHA-1 only for the following applications: hash-based message authentication codes (HMACs); key derivation functions (KDFs); and random number generators (RNGs). Regardless of use, NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.”

Wat zijn voorbeelden van implementaties van de standaard? *
> PKIoverheid, UZI-pas, boordcomputer taxi

Is het beheer van de standaard structureel geregeld? *
> Ja, zie beheerorganisaties

Impact

Welke impact (zowel positief als negatief) zou het opnemen van deze standaard als aanbevolen standaard hebben voor organisaties die deze standaard moeten invoeren? Denk

hierbij aan technische, financiële en organisatorische aspecten. *
> Er kan sprake zijn van migratiekosten, bijv. door nieuwe certificaten te implementeren en bijvoorbeeld door met oudere algoritmes gesigneerde data opnieuw te signeren.

Overige

Welke andere organisatie(s) en/of expert(s) zou(den) betrokken kunnen worden bij de beoordeling van de standaard op grond van hun expertise of anderszins? *

- PKIoverheid
- Govcert
- UZI
- KUN, Digital Security, zie: http://www.ru.nl/ds/

Wordt de standaard al voorgeschreven in wet en/of regelgeving? Zo ja, in welke wet of regelgeving *
> Ja, zie: Regeling boordcomputer taxi, bijlage 1 en 2. Zie:

- http://wetten.overheid.nl/BWBR0026626/tekst_bevat_sha/geldigheidsdatum_27-01-2010#Bijlage1
- http://wetten.overheid.nl/BWBR0026626/tekst_bevat_sha/geldigheidsdatum_27-01-2010#Bijlage2

Voorstel om een standaard van een lijst te verwijderen

Informatie over de open standaard

Volledige naam *: MD5 message-digest algorithm
Afkorting *: MD5
Versie *: April 1992
Toepassingsgebied *: Beveiliging en comprimeren van te verzenden bestanden
Beheerorganisatie *: IETF
Locatie (Website) *: http://tools.ietf.org/html/rfc1321

Een standaard van de lijst verwijderen

Op welke lijst is de open standaard te vinden? *

- Lijst met gangbare open standaarden

Waarom moet de standaard worden verwijderd?
> MD5 staat op de lijst met gangbare standaarden. Daarbij is de volgende toelichting opgenomen: "Opmerking: Hoewel defacto in gebruik, bevat de standaard fouten die tot beveiligingslekken kunnen leiden. In veiligheidskritische toepassingen wordt dan ook het gebruik van andere (nieuwere) standaarden aanbevolen."

Van verschillende kanten heeft Bureau Forum Standaardisatie commentaar ontvangen op de bovenstaande opname van MD5. Ondanks het feit dat MD5 wellicht gangbaar is, lijkt van de huidige opname van MD5 op de lijst m.b.t. informatiebeveiliging een verkeerd signaal uit te gaan.

Bovendien ontbreken op dit moment de genoemde "andere andere (nieuwere) standaarden" op de lijsten. Om dit te herstellen is bij deze melding ook de aanmelding van SHA-2 gevoegd.

Hieronder volgt relevante achtergrondinformatie:

- Uit de aanmelding van PKIoverheid blijkt dat MD5 botst met de door hen gebruikte (nieuwere) algoritmes: "Het MD5 message-digest algorithm (MD5) is niet interoperabel met met het Programma van Eisen van PKIoverheid omdat daar het SHA-1 en SHA-256 dwingend wordt voorgeschreven."
- Govcert raadt het gebruik van MD5 af en beveelt aan om gebruik te maken van de alternatieven SHA-1 en SHA-2 (zie: http://www.govcert.nl/download.html?f=122).
- En zie: http://webwereld.nl/nieuws/64342/overheid-dwingt-cruciale-standaarden-niet-af.html
- Zie onderstaande e-mail:

```
Van: [...]
Verzonden: donderdag 28 mei 2009 13:38
Aan: GBO Forumstandaardisatie
Onderwerp: md5


Geacht Forum,

Allereerst bedankt voor het goede werk aan open standaarden.
Vandaag las ik de gepubliceerde lijst met kandidaat-standaarden op http://
www.forumstandaardisatie.nl/nieuws/artikel/232/

Er staat het volgende vermeld over MD5:


Het MD5 message-digest algoritme wordt gebruik om aan de hand van de input
een 128-bit "vingerafdruk" te genereren (ofwel een 'message digest'). Er
wordt aangenomen dat het vrijwel onmogelijk is om twee berichten te laten
genereren door een computer die dezelfde vingerafdruk hebben. Het MD5
algoritme is bedoeld voor gebruik binnen digitale handtekening applicaties
waarbij een groot bestand gecomprimeerd moet worden op een veilige manier
voordat deze ge-encrypt wordt met een privé sleutel.
```

Dit klopt echter niet; MD5 is een fingerprint mechanisme en kan inderdaad gebruikt worden om een 'vingerafdruk' van een bestand te maken. Deze vingerafdruk is slechts een beperkt aantal bytes lang, terwijl het bestand wat gefingerprint is heel groot kan zijn. Een use case zou zijn als een (groot) bestand wordt overgedragen, plus de md5 fingerprint van dit bestand, na overdracht op het doelsysteem wederom een md5 checksum berekend wordt. Als deze hetzelfde is als de md5 die gegenereerd is op de broncomputer kan worden aangenomen dat het bestand 'onbeschadigd' is overgekomen.

Soms wordt het ook gebruikt als middel om wachtwoorden van gebruikers te versleutelen in databases. Niet het wachtwoord, maar de md5 sleutel van het wachtwoord wordt dan opgeslagen in de database. Als een gebruiker inlogt, berekend de applicatie de md5 waarde van het wachtwoord en vergelijkt deze met de eerder opgeslagen waarde. Als deze overeenkomt is het wachtwoord in orde en kan de gebruiker inloggen. Het voordeel is nu dat als de md5 waarden van de wachtwoorden worden ontvreemd uit de database zou er nu weinig aan de hand moeten zijn: md5 is een 'one-way' algoritme, vanuit de md5 fingerprint kan niet het oorspronkelijke wachtwoord berekend worden. Ik wil graag toevoegen dat md5 tegenwoordig niet meer als veilig beschouwd worden, er zijn allerhande mogelijkheden om vanuit een md5 sleutel toch weer een passend wachtwoord te genereren. Zie onder andere: http://www.win.tue.nl/hashclash/rogue-ca/

De Amerikaanse standaardenorganisatie NIST heeft een Secure Hash Standaard gepubliceerd: zij adviseren gebruik te maken van diverse varianten van SHA: http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf
Dat lijkt me een zinnig uitgangspunt

MD5 heeft niet direct te maken met encryptie!

Met vriendleijke groet,
--
[...]