Forum Standaardisatie

Advies ETSI TS 119 312

Datum 24 februari 2017

Analyse en Forumadvies

Het Forum Standaardisatie wordt gevraagd om in te stemmen met:

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om de aanbevolen standaard ETSI TS 102 176-1 v 2.1.1. voor het waarborgen van elektronisch handtekeningen te vervangen voor een nieuwere versie van deze standaard de ETSI TS 119 312 v1.1.1.

Aanleiding
De standaard ETSI TS 102 176-1 v 2.1.1 uit 2011 is een standaard voor het waarborgen van de authenticiteit van een elektronisch handtekening die aan een document is toegevoegd. De standaard staat op de lijst met standaarden van het Forum Standaardisatie met als status aanbevolen. Eind 2014 is deze standaard gewijzigd en vervangen voor een nieuwe versie, namelijk de ETSI TS 119 312 v1.1.1. Vanuit Logius (PKIoverheid) is het verzoek ingediend om op de lijst de 2011 versie te vervangen voor de meest recente versie van de standaard.

Over de standaard
Met ingang van de eIDAS-verordening in 2014 heeft ETSI een nieuwe set specificaties en normen uitgegeven voor elektronische handtekeningen. De Europese eIDAS verordening gaat over elektronische identificatie en het opbouwen van een Europees vertrouwenstelsel waarbinnen elkaars identificatiemiddelen worden geaccepteerd om toegang te krijgen tot (grensoverschrijdende) overheidsdienstverlening.

ETSI TS 119 312 (Electronic Signatures and Infrastructures) definieert algoritmes en sleutellengtes. De algoritmes worden gebruikt voor het plaatsen van een hash over een document of transactie en is de eerste stap naar de elektronische ondertekening van een bericht. Daarnaast geeft deze standaard een beschrijving van andere aspecten zoals algoritmen en methoden voor "signature algorithms" en "key and parameter generation algorithms".

Over de nieuwe versie
De standaard is aangepast naar aanleiding van de laatste stand van zaken van cryptografie. De uitfasering van parameters en algoritmes kan plaatsvinden als gevolg van nieuwe ontwikkelingen (pro-actief) of als gevolg van aanvallen (reactief). Daarnaast sluit de standaard beter aan op de eisen uit de eIDAS verordening en de daarin genoemd standaarden zoals de Ades Baseline Profiles (standaarden voor gekwalificeerde elektronische handtekeningen).

Ook wordt in de ETSI TS 119 312 'Whirlpool' (een cryptografie techniek) niet meer aanbevolen en is het Secure Hash Algorithm, SHA-512 vervangen door SHA-512/256.

Gebruik
Binnen Nederland is deze standaard een onderdeel van PKIoverheid. PKIoverheid levert certificaten die nodig zijn voor beveiligd internetverkeer wat gezien kan worden als een legitimatiebewijs van een website of ICT-systeem. PKIoverheid vereist dat de gebruikte lengte van cryptografische sleutels van certificaathouders conform de eisen zijn zoals gedefinieerd in ETSI TS 119 312. Internationaal wordt deze standaard ondersteund door onder andere Deutsche Telekom AG, SNG, Telenor en Uninfo.

Advies
Vervang op de lijst met aanbevolen standaarden de standaard ETSI TS 102 176-1 v. 2.1.1 door ETSI TS 119 312 v. 1.1.1.

Daarnaast wordt geadviseerd om bij toelichting op de lijst het advies op te nemen om altijd de nieuwste versie van de standaard te hanteren.

Relatie met andere standaarden
Er is een nauwe relatie met veel cryptostandaarden vanuit de aanbevelende achtergrond van de standaard, denk hierbij aan SHA.

In ETSI TS 119 312 worden bijvoorbeeld ook de minimale vereisten beschreven voor het toepassen van de hash-functie en handtekening algoritme in de Ades Baseline Profiles. Deze standaarden liggen zijn nu in procedure voor opname op de lijst met standaarden met de status 'pas toe of leg uit', zie: (https://www.forumstandaardisatie.nl/standaard/ades-baseline-profiles).

Referenties
http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf