Veelgestelde vragen fabrikanten Boordcomputer Taxi

Typegoedkeuring

#	Vraag	Antwoord
1	In paragraaf 3 (Typegoedkeuring boordcomputer) van de Regeling specificaties en typegoedkeuring boordcomputer taxi, artikel 32, eerste lid, staat dat typegoedkeuring (uitsluitend) kan worden verleend aan een boordcomputer die voldoet aan de in paragraaf 2 (Specificaties van de boordcomputer) opgenomen eisen. In paragraaf 2, artikel 17, eerste lid (De boordcomputer), onder m, l en u wordt gesteld dat de boordcomputer handtekeningen genereert op de wijzen zoals gespecificeerd in de respectievelijke paragrafen 8.5, 8.7 en 8.6 van bijlage 4. Elk van die paragrafen specificeert de door de boordcomputer te volgen stappen voor het genereren van een handtekening van een bepaald type. De stappen die alle drie de paragrafen met elkaar gemeen hebben zijn de volgende: 1.Instrueer de chip welk hash algoritme (SHA-256) hij moet gebruiken om de te ondertekenen data te hashen; 2.Instrueer de chip welk signature algoritme (PKCS#1 v1.5 – SHA-256) hij moet gebruiken om de handtekening te berekenen; 3.Bereken de (SHA-256) hash over alle input data uitgezonderd de laatste 1 tot 64 bytes en bewaar die "intermediate" hash plus het aantal gehashte input bits voor de volgende stap; 4.Instrueer de chip om de finale hash te berekenen en stuur de chip daartoe het aantal gehashte input bits, de intermediate hash en de resterende 1 tot 64 input bytes. De finale hash wordt in de chip bewaard t.b.v. het volgende en laatste chipcommando; 5.Instrueer de chip om de handtekening te berekenen (en aan de boordcomputer te retourneren) over de in de chip achtergebleven finale hash middels het commando "PSO - Create Digital Signature" (PSO-CDS) zonder verdere parameters. Wanneer bovenstaande stappen worden uitgevoerd met een bestaande BCT kaart, leidt dat tot het gewenste resultaat: een verifieerbare digitale handtekening over de input data. Wanneer bovenstaande stappen worden uitgevoerd met een BCT kaart die van de nieuwe chip is voorzien, leidt dat NIET tot het gewenste resultaat:	De tot nu toe gebruikte stappenreeks voor het met een BCT-chip genereren van handtekeningen blijft gehandhaafd, in afwachting van een chipgeneratie waarvan de tekortkoming is weggenomen. Paragrafen 8.5, 8.6 en 8.7 van bijlage 4 van de Regeling zullen elk worden uitgebreid met een bij de respectievelijke paragraaf passende variant die is gebaseerd op de tweede stappenreeks. N.B. de ILT zal de kaartproducent er op (laten) attenderen dat zij hun chips voorzien van een ATR waarmee de boordcomputer eenduidig kan vaststellen van welke chipgeneratie een BCT kaart is voorzien. Daarbij wordt onderscheid gemaakt in: 1. Een chip van de oorspronkelijke generatie die uitsluitend de eerste stappenreeks ondersteunt; 2. Een chip van de huidige generatie die beide stappenreeksen ondersteunt, maar waarbij de eerste stappenreeks verminkte handtekeningen oplevert; 3. Een chip van een toekomstige generatie die beide stappenreeksen foutloos ondersteunt. Typegoedkeuring kan uiteraard niet worden verleend indien de boordcomputer een chip van de huidige generatie aanspreekt met de eerste stappenreeks. In alle andere gevallen heeft de keuze voor eender welke (door de chip ondersteunde) stappenreeks geen effect op afgifte van typegoedkeuring.

	de chip levert zonder enige foutmeldingen een handtekening op, maar die handtekening is desondanks in veel gevallen verminkt. Dergelijke verminkte handtekeningen kunnen door geen enkel systeem (handhavingsapparatuur, software van de Belastingdienst, …) worden geverifieerd. De nieuwe BCT chip (die overigens is gecertificeerd om gebruikt te mogen worden voor het genereren van gekwalificeerde handtekeningen) ondersteunt echter een alternatieve commandoreeks die WEL leidt tot correct verifieerbare handtekeningen. De daarvoor door de boordcomputer te volgen stappen zijn dan: 1. Instrueer de chip welk signature algoritme (PKCS#1 v1.5 – SHA-256) hij moet gebruiken om de handtekening te berekenen; 2. Bereken de (SHA-256) hash over ALLE input data en bewaar die finale hash voor de volgende stap; 3. Instrueer de chip om de handtekening te berekenen (en aan de boordcomputer te retourneren) over de finale hash middels het PSO-CDS commando waarbij de finale hash als parameter wordt meegestuurd aan de chip. Ter illustratie van de verschillen tussen de eerste en de tweede stappenreeks is een grafisch overzicht als bijlage 1 ingesloten. De nieuwe BCT chip is gecertificeerd om gebruikt te mogen worden voor het genereren van gekwalificeerde handtekeningen conform Europese regelgeving; ongeacht welke van de twee bovengenoemde stappenreeksen wordt toegepast (en ondanks het feit dat de eerstgenoemde stappenreeks in de praktijk vaak leidt tot niet-verifieerbare handtekeningen). Bijlage 4 van de huidige Regeling specificeert echter uitsluitend de eerstgenoemde stappenreeks. Mogen wij desondanks - en zonder negatieve gevolgen voor de typegoedkeuring - van de tweede stappenreeks gebruik maken, zodat we niet alleen aan de Europese regelgeving voldoen, maar ook daadwerkelijk verifieerbare (niet-verminkte) handtekeningen kunnen genereren?	