

## **Beantwoording IAK-vragen bij Besluit beveiligde verbinding met overheidswebsites en -webapplicaties**

### **1. Wat is de aanleiding**

De minister van Binnenlandse Zaken en Koninkrijkrelaties heeft de Tweede Kamer in februari 2017 toegezegd de toepassing van de HTTPS-standaard bij overheidswebsites te zullen verplichten. Deze standaard zorgt voor een beveiligde verbinding van gebruikers met overheidswebsites (het kenmerkende slotje in de adresbalk van de internetbrowser).

### **2. Wie zijn betrokken**

- Overheidsorganisaties
- Nationaal Cyber Security Centrum (NCSC)
- Forum Standaardisatie

### **3. Wat is het probleem**

Met de groei van de afhankelijkheid van het internet zijn de risico's voor de veiligheid en privacy van bezoekers van websites eveneens toegenomen. Ieder internetgebruik dat bijvoorbeeld niet via HTTPS verloopt geeft informatie over het gedrag van de gebruiker en kan interessant zijn voor derden om te verzamelen. Het is daarom belangrijk dat bestuursorganen hun websites goed beveiligen.

### **4. Wat is het doel?**

Gebruikers van overheidswebsites moeten erop kunnen vertrouwen dat informatie-uitwisseling vertrouwelijk verloopt doordat de verbinding met website beveiligd is, dat de informatie van de website daadwerkelijk afkomstig is van de beheerder van de website en dat de website daadwerkelijk hoort bij de gebruikte domeinnaam.

### **5. Wat rechtvaardigt de overheidsinterventie?**

De verplichtstelling is het sluitstuk op ingezet beleid. Voor de HTTPS- en HSTS-standaard geldt momenteel het zogenaamde pas-toe-of-leg-uit-beleid voor open standaarden. Dit beleid houdt kort gezegd in dat op het moment dat een overheidsorganisatie investeert in een ICT-systeem of -dienst, de relevante standaarden van de pas-toe-of-leg-uit-lijst van Forum Standaardisatie moeten worden toegepast. Nu hebben overheidsorganisaties nog de mogelijkheid af te wijken van de voorgeschreven standaarden indien hiervoor een zwaarwegende reden is. Met dit besluit verdwijnt die mogelijkheid.

### **6. Wat is het beste instrument?**

De Wet digitale overheid biedt in artikel 3 de mogelijkheid dat bij algemene maatregel van bestuur (amvb) open standaarden aanwijst ten behoeve van verplichte toepassing indien dit proportioneel is gelet op de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid en de doelmatigheid van het elektronisch verkeer.

### **7. Wat zijn de (neven)gevolgen voor burgers, bedrijven, overheid en milieu?**

De verplichting om HTTPS en HSTS toe te passen op overheidswebsites heeft geen (financiële) gevolgen voor burgers en bedrijven. Alle gangbare versies van de internetbrowsers, zoals Chrome, Safari, Firefox en Internet Explorer, ondersteunen de standaarden. Burgers en bedrijven hoeven niets te doen om van het voordeel van een veilige, privacybeschermende verbinding met een overheidswebsite te kunnen profiteren.

Voor overheidsorganisaties die de standaarden nog niet toepassen heeft het besluit tot gevolg dat de standaarden moeten configureren op de webserver en TLS-certificaten toepassen.