Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

31 700 VII Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2009

Nr. 56

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 december 2008

Met excuses voor de late beantwoording, bied ik u hierbij conform mijn toezegging in het AO van 2 oktober, grote ICT-projecten (Kamerstuk 30 146/26 643, nr. 23H), mijn antwoord op de vraag van het Kamerlid Gerkens (SP) over de openheid van de chiptechnologie in de Rijkspas aan. De brief met antwoord was wel al veel eerder opgesteld, maar om onduidelijke redenen niet verzonden.

Het antwoord ten aanzien van de openheid van de broncode van de chiptechnologie is dat de chiptechnologie voor de toegangsverlening met de rijkspas bestaat uit verschillende elementen.

De communicatie lagen zijn gebaseerd op internationale standaarden voor contactloze toepassingen (ISO/IEC-14443A). Dit zijn open standaarden.
De contactloze chip maakt gebruik van een publiekelijk bekend encryptiealgoritme die als standaard erkend is en waarover in de publieke literatuur uitvoerige analyses beschikbaar zijn. De specifieke wijze waarop de algemeen erkende standaarden geïmplementeerd zijn c.q. worden door de chipleverancier in de contactloze chip zijn niet openbaar en van dit specifieke deel is derhalve géén broncode beschikbaar.

Het bovenstaande vormt een groot contrast met de Mifare Classic chip. De hierin toegepaste cryptografische algoritmen waren niet publiekelijk bekend, werden niet vrijgegeven door de leverancier en waren daarom ook niet verifieerbaar voor externe partijen.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst

KST126723
0809tkkst31700VII-56
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2009