Management samenvatting van het belang van een PKI voor C-ITS

Waar hebben we het over als we spreken over C-ITS en PKI?

- Voor vele coöperatieve ITS-services (C-ITS) zijn er vertrouwensrelaties nodig tussen deelnemers in het verkeer (V2X) of tussen verkeersdeelnemers en de wegbeheerder (V2I, I2V). Daarmee kunnen partijen op vertrouwde wijze berichten met elkaar uitwisselen en eventuele transacties verrichten.
- Kenmerkend in C-ITS is dat partijen in het verkeer elkaar niet kennen (zoals voertuigen en verkeersregelinstallaties) en direct en tijdelijk iets voor elkaar kunnen betekenen.
- De vertrouwensrelatie tussen twee partijen kan instantaan tot stand worden gebracht via een derde partij die door beide partijen vertrouwd wordt, een zogenaamde Trusted Third Party.
- Een van de technische en organisatorische middelen die de vertrouwde derde partij kan inzetten is een PKI.

Wat is PKI?

- PKI staat voor een Public Key Infrastructure. Dit is een afsprakenstelsel dat technisch wordt mogelijk gemaakt door het gebruik van cryptografie.
- Met een PKI kunnen partijen die iets met elkaar willen delen - maar elkaar niet kennen – een tijdelijke vertrouwensrelatie opbouwen.
- PKI's worden wereldwijd in vele bedrijfssectoren toegepast omdat zij erg betrouwbaar en schaalbaar zijn voor grote toepassingen met vele gebruikers. Vele belangrijke diensten via het internet maken gebruik van PKI.
- De PKI wordt organisatorisch en technisch beheerd door een organisatie die door de betrokkenen wordt vertrouwd, met vele onderscheidende rollen en taken.

Wat zijn de vertrouwenseigenschappen die een PKI kan bieden aan C-ITS-services?

- integriteit – de zekerheid voor de verzender en de ontvanger van een C-ITS-bericht dat de inhoud van het bericht identiek wordt afgeleverd als het is verstuurd – van belang voor alle C-ITS-services.
- vertrouwelijkheid – de zekerheid voor de verzender dat de inhoud van een C-ITS-bericht alleen toegankelijk is voor de bedoelde ontvanger – bij C-ITS-services m.n. van belang bij berichttypes waar *privacy* een rol speelt.
- autorisatie – de zekerheid voor de ontvanger van een C-ITS-bericht dat de andere partij bevoegd is voor de bijbehorende C-ITS-service – speelt voor alle C-ITS-services.
- authenticatie – de zekerheid voor de ontvanger van de identiteit van de verzender (bij I2V). Bij V2X is in het bericht de identiteit van de verzender afgeschermd vanwege het belang van privacy van de verkeersdeelnemer. De zekerheid die de ontvanger dan gegeven wordt, is dat de autorisatie gekoppeld is aan de echte identiteit van de verzender (V2X).
- juridische zekerheid – een juridisch bewijs van de verzending, de inhoud en de ontvangst van een C-ITS-bericht door betrokkenen – te bepalen door de eindverantwoordelijke ITS-dienstverlener.

Welke alternatieven bestaan er voor het gebruik van PKI?

- C-ITS-services kunnen ook gebruik maken van bestaande cellulaire netwerken (3/4G) van Mobiele Netwerk Operators (MNO's) gebruiken (zoals KPN, Vodafone, T-Mobile) en de daarvoor ontwikkelde security oplossingen, zoals secure SIM-kaarten. Aan de hand van de onderstaande lijst van criteria kan voor een bepaalde C-ITS-service worden bepaald of een PKI noodzakelijk is.
- Innovaties als Attribute Based Credentials (ABC) en Blockchain zijn nog te weinig doorontwikkeld voor grootschalige toepassing binnen C-ITS binnen enkele jaren.

Beoordeling van alternatieven voor een PKI voor C-ITS-services

- Eisen aan het uitgifteproces – Hoe dient de identiteit van de aanvrager van een C-ITS-service te worden vastgesteld en vastgelegd? Welke eisen voor betrouwbaarheid en toezicht gaan gelden voor het de processen van registratie, autorisatie en uitgifte? Hebben C-ITS-services specifieke eisen of volstaan de betreffende processen en registraties van MNO's?
- Eisen aan het sleutelbeheer – Hoe vertrouwelijk gaan deelnemers hun geheime sleutel-materiaal uitwisselen? Wordt de hoogste eis gesteld dat geheim sleutel-materiaal met helemaal niemand wordt gedeeld, dan komt alleen een PKI in aanmerking. Het al dan niet stellen van deze eis is de uitkomst van de hardheid van de bovenstaande 5 vertrouwenseigenschappen voor een specifieke C-ITS-dienst.
- Technologie-neutraliteit – Security diensten van MNO's werken alleen indien gebruik wordt gemaakt van hun netwerkdiensten ter plaatse voor de C-ITS-dienst. Een PKI is technologie-neutraal en kan worden toegepast in zowel cellulaire connectiviteit, LTE-V2X als Wifi-P (G5).
- Geografische dekking – C-ITS-diensten die volledige geografische dekking willen geven, ook indien er geen of onvoldoende cellulaire dekking is, zullen ook andere connectiviteitsopties bieden en waar nodig dynamisch switchen tussen netwerken en netwerk-technologieën. Een PKI geeft door zijn technologische neutraliteit een grotere geografische dekking.
- Duurzaamheid en portabiliteit – Op dit moment zijn SIM-kaarten veelal gekoppeld aan abonnementen van Mobiele providers. Dit kan in de nabije toekomst snel gaan veranderen door de grootschalige introductie van zgn. eSIM's in mobiele devices.

Welke Trusted Third Parties komen in aanmerking voor een PKI in C-ITS?

- Bestaande PKI's voldoen niet aan alle eisen van C-ITS, zoals het optimale gebruik van het radiospectrum (bij gebruik van Wifi-P/G5 technologie), en wettelijke eisen van data protectie (privacy) indien gebruikt voor C-ITS-services.
- Voor C-ITS wordt momenteel een gezamenlijke PKI ingericht door de EC i.s.m. de lidstaten, de auto-industrie en de toeleveranciers. Deze ITS-PKI zal bruikbaar zijn in de gehele EU en is technologie-neutraal. De governance van de ITS-PKI zal liggen bij alle genoemde stakeholders. De gezamenlijke ITS-PKI zal bestaan uit meerdere trusted third parties (TTP's) die onderling interoperabel zullen zijn en een gelijk niveau van accreditatie zullen kennen.

- Op dit moment is nog niet bepaald welke TTP gebruikt zal gaan worden door Nederlandse verkeersdeelnemers en Nederlandse weginfrastructuur. Evenmin is bepaald of en hoe Nederland een eigen TTP gaat inrichten t.b.v. de ITS-PKI.