PIN B.V.

BIJLAGE – J

Rules & Regulations bepalingen

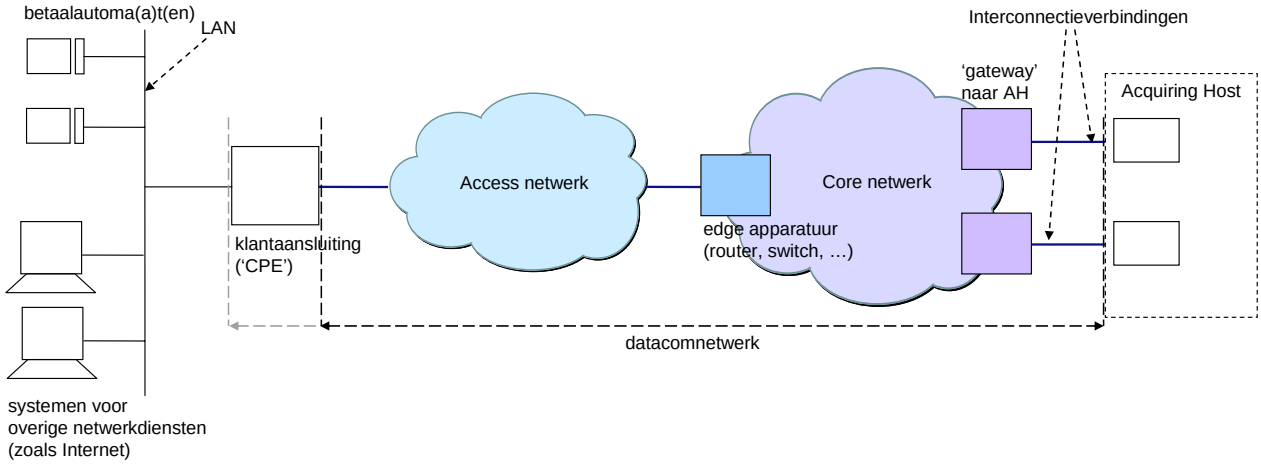
Generieke eisen ten aanzien van datacomnetwerken voor het transport van het PINbetalingsverkeer

Versie : 3.2
Datum : januari 2009

Inhoudsopgave

1 INLEIDING

Het datacomnetwerk van de Datacomleverancier, dat gebruikt wordt voor het transport van electronisch betalingsverkeer tussen de terminal bij een Acceptant en de Acquiring Host bij een Acquiring Processor, heeft in het algemeen de volgende configuratie (zie Figuur 1).



Figuur 1. Schematisch overzicht van het datacomnetwerk, dat de betaalautomaataansluiting op de lokatie van de Acceptant (klant) verbindt met de Acquiring Host. De klantaansluiting kan zowel binnen als buiten het domein van de Datacomleverancier vallen.

In dit document worden de technische eisen beschreven die PIN B.V. stelt aan datacomnetwerken. Hoewel op enkele punten verschillende eisen worden gesteld aan verschillende netwerkdelen, kan een Datacomleverancier alleen voor het gehele datacomnetwerk een certificaat van PIN B.V. ontvangen. Deelcertificaten worden niet verstrekt.

Opmerking 1: Bij een aantal van de in dit document genoemde eisen zijn geen concrete toetsingsnormen gegeven. Bij toetsing van deze eisen zal aannemelijk moeten worden gemaakt, dat het datacomnetwerk van de Datacomleverancier aan deze eisen voldoet.

Opmerking 2: Het kan voorkomen dat de apparatuur (router, switch, SIM-kaart, …) op lokatie van de Acceptant niet in eigendom en/of beheer is van de Datacomleverancier. Aangezien de technische eisen bewust *inclusief* deze apparatuur gesteld zijn, zal de Datacomleverancier in een dergelijk geval afspraken moeten maken met de Acceptant over de performance hiervan.

Opmerking 3: Het kan voorkomen, dat zich achter de klantaansluiting een Wide Area Network (WAN) van de Acceptant bevindt, dat beheerd wordt door de Acceptant zelf of een door deze ingeschakelde derde partij. Aangezien de technische eisen *inclusief* het WAN gesteld zijn, zal de Datacomleverancier in een dergelijk geval afspraken moeten maken met de Acceptant over de performance hiervan.

2 EISEN AAN HET DATACOMNETWERK

2.1 Inleiding

De eisen die PIN B.V. aan datacomnetwerken stelt, hebben betrekking op de Transactietijd, Beschikbaarheid en Security van de dienstverlening door de Datacomleverancier. Sommige eisen zijn afhankelijk van de situatie waarin de PINdienst wordt geleverd. PIN B.V. onderscheidt hiertoe de volgende toepassingscategorieën:

Categorie 1	Categorie 2
Vast opgestelde PIN-terminal(s)	Mobiele, draadloze PIN-terminal (b.v. voor betalingen aan de deur)

Tabel 1. Overzicht van door PIN B.V. onderscheiden toepassingscategorieën voor de PINdienst.

2.2 Beschrijving Eisen

2.2.1 Transactietijd

Eis T01:
Minimaal 95% van alle PIN-transacties tussen terminal en Acquiring Host (AH) is voltooid binnen x seconden, exclusief de bijdragen aan deze transactietijd door terminal en AH. (Het gaat dus puur om de bijdrage van het datacomnetwerk aan de transactietijd.) De waarde van x is afhankelijk van de toepassingscategorie, zie onderstaande tabel.

Categorie	x
1	1,0
2	2,0

Tabel 2. Overzicht van de eisen per toepassingscategorie aan het 95%-percentiel van de transactietijd.

Toelichting:
PIN B.V. wil haar eisen aan Datacomleveranciers niet blokkerend voor technologische innovaties maken en daarom zijn deze technologie-onafhankelijk geformuleerd. Voor de huidig voorkomende IP- en X.25-protocollen geldt dat Eis T01 zich praktisch gezien als volgt laat vertalen:

- IP:
  1 maal de round trip delay (tussen terminal en AH) gemeten door een ICMP bericht van 32 Bytes, plus 1 maal de round trip delay gemeten door een ICMP bericht van 144 Bytes,
  dient korter dan x seconden te zijn in minimaal 95% van de gevallen.
- X.25:
  De Call Set-up Delay plus de Data Transfer Delay dient korter dan x seconden te zijn in minimaal 95% van de gevallen.

Eis T02:
De Datacomleverancier dient een deugdelijk capaciteit- en voorraadmanagementproces ingericht te hebben, met als doel om te allen tijde – dus ook tijdens zware belasting van het netwerk – aan Eis T01 te voldoen.

Toelichting:
Onderdeel hiervan is bijvoorbeeld het stellen van maximaal toegestane verkeersbelastingen op alle netwerklinks, het bewaken of deze overschreden worden en het tijdig ingrijpen wanneer dit dreigt te gebeuren.

Eis T03 (alleen in het geval van datacomnetwerken waarover naast PIN nog meer diensten worden aangeboden aan de Acceptant):
Aanvullend aan Eisen T01 en T02 geldt dat de Datacomleverancier Pinverkeer op de access line naar de Acceptant middels (een) Traffic Management mechanisme(s) moet beschermen tegen (door de Acceptant zelf veroorzaakte) congestie in de downstream richting.

Toelichting:
Voorbeelden van Traffic Management[1] mechanismen zijn het toepassen van queuing mechanisme in de edge router/switch en het gebruiken van verschillende ATM VC's voor PIN- en overig verkeer, waarop policing/shaping en Connection Admission Control toegepast wordt.

Eis T04:
Indien in het netwerk van de Acceptant (op de winkelaansluiting) geen mechanismen zijn geïmplementeerd die PIN verkeer beschermen tegen congestie in de upstream richting, dient de Datacomleverancier de Acceptant degelijk voor te lichten over het effect van mogelijk door hemzelf veroorzaakte congestie op de access line.

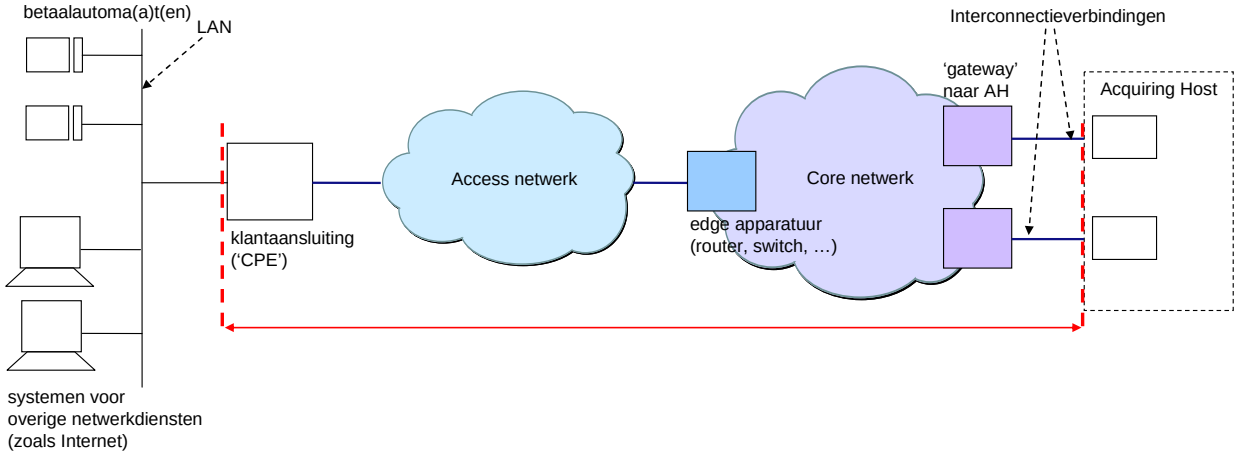
[1] Naast 'Traffic Management' wordt ook wel de term 'QoS differentiatie' gebruikt.

2.2.2 Beschikbaarheid

Eis B01:

Voor toepassingen uit Categorie 1 (zie paragraaf 2.1):

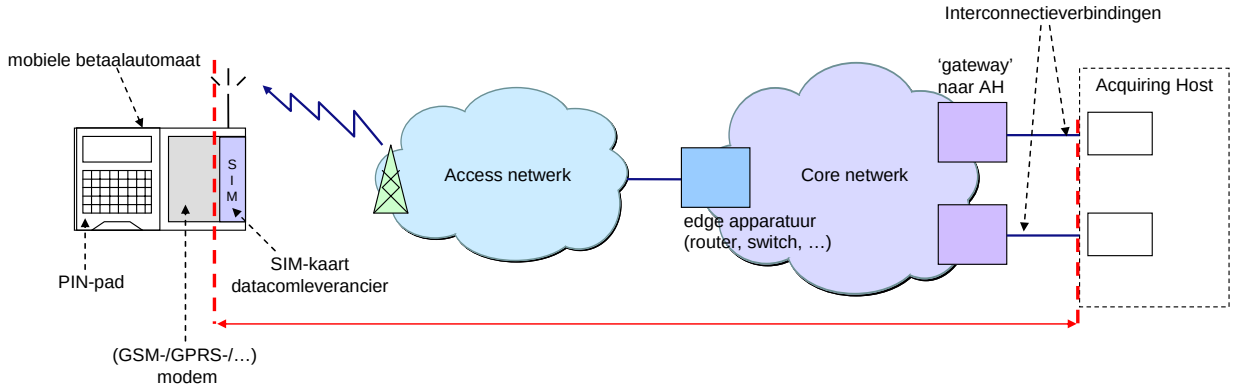
De beschikbaarheid van verbindingen tussen het koppelvlak betaalautomaat – klantaansluiting (CPE) en het koppelvlak core netwerk – Acquiring Host (zie dubbele pijl in Figuur 2) is minimaal 99,6% op jaarbasis.



Figuur 2. Schematisch overzicht van het datacomnetwerk, dat de betaalautomaataansluiting op de lokatie van de Acceptant (klant) verbindt met de Acquiring Host. De stippellijnen geven de interfaces aan waarop Eis B01 is gedefinieerd.

Voor toepassingen uit Categorie 2:

De beschikbaarheid van verbindingen tussen het koppelvlak PINpad – SIM-kaart en het koppelvlak core netwerk – Acquiring Host (zie rode dubbele pijl in Figuur 3) is minimaal 99,6% op jaarbasis.



Figuur 3. Schematisch overzicht van het datacomnetwerk, dat de SIM-kaart in de mobiele betaalautomaat van de Acceptant (klant) verbindt met de Acquiring Host. De stippellijnen geven de interfaces aan waarop Eis B01 is gedefinieerd.

Toelichting:
'Beschikbaarheid' is hier gedefinieerd als het percentage van de tijd waarin:
1) verbindingen mogelijk zijn tussen betaalautoma(a)t(en) en (uitsluitend) de bijbehorende Acquiring Host;
2) hierover PINtransacties succesvol uitgevoerd kunnen worden.

Noot: met 'tijd' wordt hier de tussen Acceptant en Datacomleverancier overeengekomen periode bedoeld waarbinnen het netwerk geschikt – en dus gecertificeerd – voor Pinverkeer moet zijn. Dit kan bijvoorbeeld 24x7 uur per week (continu) gelden, in- of exclusief gepland onderhoud, maar ook alleen tijdens winkeltijden.

Eis B01A (alleen voor toepassingen uit Categorie 2):
Aanvullend aan Eis B01 dient de Datacomleverancier de Acceptant degelijk voor te lichten over het dekkingsgebied van het mobiele netwerk, waarbinnen betaaltransacties succesvol mogelijk zijn volgens de eisen van Currence.

Eis B02:
Aanvullend aan Eis B01 geldt een toegestane storingsduur (Time To Repair) voor een enkele storing. Deze is afhankelijk van het netwerkniveau binnen het datacomnetwerk en wordt gegeven door onderstaande tabel.

Type storing	**Duur (Time To Repair) van een enkele storing**
CPE	100% < 16 kantooruren
Local loop (i.g.v. Cat. 1) of Radio netwerk (i.g.v. Cat. 2)	80% < 24 uur; 90% < 48 uur
Edge-router	100% < 8 uur
Core-netwerk	100% < 4 uur

Tabel 3. Overzicht van de eisen aan maximale storingsoplossingstijd, afhankelijk van het netwerkniveau.

Eis B03:
Aanvullend aan Eisen B01 en B02 geldt dat het Interconnectienetwerk volledig redundant moet zijn uitgevoerd. Dat wil zeggen dat de gebouwen, apparatuur binnen die gebouwen (routers, switches etc.) en de transmissielijnen (glasvezels/coax/koper) dubbel en geografisch volledig gescheiden moeten zijn uitgevoerd.

2.2.3 Security

Eis S01:
Datacomleveranciers dienen ervoor zorg te dragen dat verbindingen volgens de correcte paden tot stand komen.

Eis S02:
Datacomleveranciers dienen ervoor te zorgen dat de transactiestroom door geen andere partij kan worden gezien of benaderd dan de PINterminal en de Acquiring Host.

Eis S03:
Datacomleveranciers dienen ervoor te zorgen dat noch de PINterminal, noch de Acquiring Host kan worden gezien of benaderd door andere partijen dan de Acceptant en de Acquiring Processor.

Eis S04:
De Interconnectiekoppeling mag alleen voor PIN- en terminalmanagementverkeer worden gebruikt.

Eis S05:
De netwerkelementen die gebruikt worden om Pinverkeer te routeren mogen slechts het verkeer doorrouteren en mogen zelf niet benaderbaar zijn, behalve door de netwerkbeheerders van de datacomleverancier.

Eis S06:
De Datacomleverancier dient ervoor te zorgen dat in het beheernetwerk een terminalmanager opgezet kan worden die door de Terminalleveranciers van buiten het netwerk van de Datacomleverancier benaderbaar is. De terminals dienen binnen het netwerk van de Datacomleverancier op eigen initiatief connectie te kunnen maken met de terminalmanager.

Eis S07:
Het is niet toegestaan getransporteerde data op welke wijze dan ook te dupliceren en op te slaan.

Eis S08:
Het beheernetwerk van de datacomleverancier dient een logisch gescheiden netwerk te zijn.

Eis S09:
De netwerkbeheerders dienen te werken volgens een vastgesteld autorisatiemodel.

Eis S10:
Iedereen die volgens het autorisatiemodel toegang heeft tot netwerkelementen dient een vastgesteld identificatie- / authenticatie-proces te doorlopen.

Eis S11:
Datacomleveranciers zijn verplicht de netwerkbeheerders in de aannameprocedure te onderwerpen aan een screening.

Eis S12:
Datacomleveranciers dienen het beheer dusdanig te hebben ingericht dat adequaat op beveiligingsincidenten kan worden gereageerd.

Eis S13:
Zowel de lokatie van waaruit netwerkbeheer wordt verricht als de netwerkelementen zelf dienen in een meerlaags beveiligingsmodel te zijn afgeschermd.

Eis S14:
Toegepaste bekabeling en apparatuur dienen te voldoen aan de daarvoor geldende (internationale) standaards.

Eis S15:
Het netwerk van de datacomleveranciers dient te bestaan uit correct onderhouden apparatuur.

Eis S16:
Wijzigingen in het netwerk dienen te worden beheerd en te zijn gedocumenteerd.

Eis S17:
Datacomleveranciers dienen preventieve maatregelen te hebben getroffen tegen kwaadaardige software.