Regelgeving

Betaalvereniging Nederland

Procedure Security Certificering Betaalautomaten

Versie 2.01 | 7 april 2015 | proc.cert.betaalautomaten

Betaalvereniging Nederland

Inhoudsopgave

Versie historie

Versie nummer	Versie datum	Status	Gewijzigd door	Meest belangrijke wijziging(en)
1.0	*11-04-2012*	*definitief*	*Betaalvereniging*	
1.1	*11-07-2012*	*definitief*	*Betaalvereniging*	*Regels voor PCI-only betaalautomaten toegevoegd; versienrs van document verwijderd (verwijzing naar meest recente)*
1.2	*11-10-2012*	*definitief*	*Betaalvereniging*	*Procedure voor non-pincode betaalautomaten toegevoegd (aparte bijlage)*
1.3	*14-03-2013*	*definitief*	*Betaalvereniging*	*Nadere toelichting op periodieke herbeoordeling (par 3.4 en 3.5)*
2.0	*25-02-2015*	*Draft*	*Betaalvereniging*	*Herijking* *Verplichte ondersteuning SRED voor nieuwe certificeringen per 1-1-2016;* *Procedure voor integreren betaalterminal in vending machine toegevoegd;* *Acquirer informeren over opbouw betaalketen van POI tot aan de acquirer processor.*
2.01	*7-04-2015*	*definitief*	*Betaalvereniging*	*Review commentaar verwerkt*

1. Algemeen

In deze procedure ‘Security Certificering Betaalautomaten’ worden de voorwaarden beschreven waaraan leveranciers en/of fabrikanten van betaalautomaten moeten voldoen om in aanmerking te komen voor een bewijs van goedkeuring. Het bewijs van goedkeuring wordt verstrekt door de Betaalvereniging (hierna te noemen de Betaalvereniging) en is nodig voor in Nederland geplaatste betaalautomaten waar de bijbehorende acquirers lid zijn van de Betaalvereniging (http://www.betaalvereniging.nl/leden/).

Onder een leverancier wordt verstaan een onderneming (leveranciers en/of fabrikanten van betaalautomaten) die, conform de eisen van de Betaalvereniging, betaalautomaten levert voor aansluiting op de betaalinfrastructuur voor elektronisch betalen in Nederland.

1.1 Certificeringsentiteit

De Betaalvereniging zal in dit kader, in haar rol van certificeringsentiteit, de certificeringswerkzaamheden verrichten. Deze werkzaamheden zullen in lijn met Europese ontwikkelingen de volgende taken omvatten voor betaalautomaten op de Nederlandse markt:

1. Het onderhouden van de certificeringsprocedure voor betaalautomaten;
2. Het verstrekken van een bewijs van goedkeuring / security certificaat voor een betaalautomaat, voor aansluiting op de betaalinfrastructuur voor elektronisch betalen, na het succesvol doorlopen van de certificeringprocedure;
3. Het publiceren van goedgekeurde betaalautomaten op de daarvoor bestemde website;
4. Het in kaart (laten) brengen van de achterliggende betaalketen. Met achterliggende betaalketen wordt de infrastructuur bedoeld van gecertificeerde betaalautomaat tot aan de verwerkende systemen van de acquiring host processor.
5. Het voeren van het risicobeheer met betrekking tot goedgekeurde operationele betaalautomaten en achterliggende betaalketen waaronder begrepen:
   - Het beheer van de levenscyclus van verstrekte goedkeuringen (aflopen van goedkeuringen o.b.v. eerder verstrekte security certificaten)
   - Het monitoren van (en opvolging geven aan) incidenten in het veld (o.a. als fraude management)
   - Het rapporteren van eventuele risico’s in de betaalketen aan verantwoordelijke acquirer(s).
6. Het volgen van de Europese ontwikkelingen op het gebied van certificering en het behartigen van de belangen van de leden ter zake.

1.2 Scope

De scope van deze certificeringsprocedure beperkt zich tot security certificering van betaalautomaten en het integreren van een onbemande betaalautomaat in een vending machine. De procedure is geënt op de oude PCI+ certificeringsprocedure voor PIN, maar houdt rekening met Europese eisen voor certificeringsprocessen zoals beschreven Book 4 van de EPC Volume. In Bijlage 1 Test- en Certificeringsmodel Betaalautomaten wordt ter illustratie het totaal aan certificeringen die Nederlandse betaalautomaat doorgaans doorloopt geschetst inclusief dit certificeringsproces.

1.3 Certificering van non-pincode betaalautomaten

De procedure ‘Security Certificering Betaalautomaten’ zoals hierboven geschetst heeft betrekking op betaalautomaten waarbij voor het doen van een betaaltransactie een pincode wordt ingevoerd. Marktontwikkelingen hebben er voor gezorgd dat ook betaalautomaten zonder ondersteuning van pincode invoer beschikbaar zullen komen. (Bv. Dip & go betaalautomaten in de parkeersector) Ook voor deze betaalautomaten geldt een certificeringsplicht. Omdat deze betaalautomaten echter een ander (security) risico profiel hebben, zal voor deze non-pincode betaalautomaten een afwijkende certificeringsprocedure worden gehanteerd. Deze certificeringsprocedure is beschreven in Bijlage 7.

1.4 Beoordelen Privacy Shield

Met uitzondering van betaalautomaten die voldoen aan de criteria die gelden voor een handheld volgens de PCI standaard moeten alle betaalautomaten voor de Nederlandse markt beschikken over een privacy shield die voldoet aan “EPC343-08 PRIVACY SHIELDING FOR PIN ENTRY” Versie 1.4 van 30 September 2009. Voor onbemande betaalautomaten is het toegestaan dat pas bij het integreren van de betaalautomaat in de Vending Machine voldaan wordt aan de privacy shield eisen. Deze procedure is beschreven in Bijlage 8**.**

1.5 Opzet document

In *hoofdstuk 1,* dit hoofdstuk is algemene uitleg gegeven, de betrokken partijen beschreven en toegelicht voor welke betaalautomaten deze certificeringsprocedure geldt en wat de scope is van het certificeringsprogramma*.*

In *hoofdstuk 2* wordt een overzicht gegeven van de certificeringsprocedure inclusief een verwijzing naar van toepassing zijnde eisen.

In *hoofdstuk 3* wordt de procedure in stappen weergegeven die specifiek voor de Nederlandse markt van toepassing zal zijn.

2. Overzicht voor het verkrijgen van een bewijs van goedkeuring

Het bewijs van goedkeuring dat de Betaalvereniging afgeeft voor de security certificering van betaalautomaten is gebaseerd op de Europese eisen zoals gepubliceerd door de EPC in Book 4 van de SCS Volume. De fysieke en logische PCI eisen afkomstig uit de PCI PTS standaard vormen de basis voor de Europese eisen, in aanvulling hierop gelden EPC PLUS eisen voor veilige afhandeling van de betaaltransactie en eisen voor productieproces van de betaalautomaat. Voor een nadere beschrijving van deze Europese eisen (naar onderliggende versie van de PCI standaard) wordt verwezen naar Bijlage 2.

Vanaf 1-1-2016 geldt de aanvullende eis dat betaalautomaten die aangeboden worden voor een initiële certificering, gebruik moeten maken van Secure Reading and Exchange of Data (SRED). De te gebruiken SRED module moet door PCI SSC gecertificeerd zijn in combinatie met key management schema dat voor de Nederlandse markt gebruikt wordt. Voor delta certificeringen geldt een overgangstermijn van 12 maanden. Dit geldt niet voor de betaalautomaten waarvoor SRED niet beschikbaar is zoals PCI PED 1.3 en 2.* gecertificeerde betaalautomaten.

Als bewijs dat aan de PCI eisen is voldaan, dient de leverancier een PCI certificaat en het onderliggende evaluatierapport op te leveren aan de Betaalvereniging. Inzage in het evaluatierapport is noodzakelijk voor het risicobeheer, een van de taken die horen bij de rol van een certificeringsentiteit.

Als bewijs dat aan de EPC PLUS eisen is voldaan, dient de leverancier evaluatierapporten aan te leveren. Deze evaluatierapporten dienen verslag te doen van het onderzoek naar de EPC PLUS eisen en mogen alleen opgesteld worden door daartoe door de Betaalvereniging geaccrediteerde evaluatielaboratoria. De evaluatierapporten worden vervolgens door de Betaalvereniging beoordeeld op juistheid en volledigheid om te komen tot een bewijs van goedkeuring.

Het PCI certificaat en de certificering van de betaalautomaat volgens de EPC PLUS eisen door de Betaalvereniging, resulteert in een bewijs van goedkeuring. De leverancier ontvangt een bewijs van goedkeuring per brief, die ondertekend is door de directie van de Betaalvereniging.

3. Proces

Vereist voor de betaalautomaatcertificering is de aanwezigheid van een ondertekende Standaardovereenkomst betaalautomaatleverancier waarin de afspraken zijn vastgelegd tussen enerzijds de Betaalvereniging en anderzijds de leverancier.

De Betaalvereniging is het aanspreekpunt voor de leverancier die zijn betaalautomaat laat certificeren. Hierbij zijn de volgende fases te onderkennen:

1. Het aanmelden door de Leverancier bij de Betaalvereniging (gegevens leverancier en betaalautomaat).
2. Het vastleggen van de betaalketen, vanaf betaalautomaat tot aan de transactie verwerkende systemen van de acquirer processor indien van toepassing. Doel is inzicht te verkrijgen aan welke relevante normen voldaan wordt door de diverse componenten alsmede hoe de diverse componenten data met elkaar uitwisselen.
3. Het beoordelen van de, door de leverancier beschikbaar gestelde, onderzoeksrapporten (over de eerder genoemde aandachtsgebieden) door de Betaalvereniging.
4. Het verstrekken van een bewijs van goedkeuring door de Betaalvereniging. Goedgekeurde betaalautomaten worden gepubliceerd op de website van de Betaalvereniging

3.1 Aanmelding betaalautomaat en registratie betaalketen

De Betaalvereniging is het aanspreekpunt voor de leverancier die zijn betaalautomaat laat certificeren. De Betaalvereniging zal ook helpen bij het coördineren van de deelonderzoeken in het kader van de certificering. Naast nieuwe betaalautomaten dienen ook betaalautomaten aangemeld te worden waarop wijzigingen zijn doorgevoerd die van invloed (kunnen) zijn op de security aspecten van de betaalautomaat. (zie Bijlage 2). Doel van de aanmelding is het registreren van de ter certificering aangeboden betaalautomaat en het over en weer verstrekken van alle noodzakelijke informatie en benodigdheden voor uitvoeren van een certificering.

De leverancier dient verder inzicht te geven in de achterliggende betaalketen. Dit door invullen van de Conformiteitsverklaring zoals beschreven in Bijlage 6.

3.2 Scope van het onderzoek

Na overleg met de leverancier zal door de Betaalvereniging de scope worden bepaald op basis waarvan een evaluatielaboratorium haar onderzoek zal verrichten. De leverancier kan hierbij kiezen voor een van de evaluatielaboratoria zoals opgenomen in Bijlage 10.

Indien sprake is van een nieuw type betaalautomaat zal een volledige certificering worden uitgevoerd. In geval van wijzigingen op een bestaand type betaalautomaat zal alleen de impact beoordeeld te worden en hoeft slechts een deel van de certificeringsprocedure doorlopen te worden.

Specifiek voor wijzigingen in de security software wordt nader onderscheid gemaakt in wijzigingen met grote impact en kleine wijzigingen.

Wijzigingen betreffende de security software van de betaalautomaat met mogelijk grote impact dienen eerst ter beoordeling worden voorgelegd aan de Betaalvereniging. Pas na goedkeuring mogen deze wijzigingen operationeel in gebruik worden genomen. Of er sprake is van een mogelijke grote impact dient te worden bepaald middels een risicoanalyse. Hierbij moet in ieder geval worden gekeken naar alle functionaliteit welke verantwoordelijk is voor afhandeling van de pincode en/of bijbehorend key-management. Wijzigingen in pincode afhandeling en key management worden altijd aangemerkt als wijzingen met grote impact.

Voor kleine wijzigingen is de procedure anders. Leveranciers zijn in dat geval gerechtigd om kleine wijzigingen in de security software van de betaalautomaat door te voeren. Voorwaarde is dat de Betaalvereniging voor ingebruikname in de operationele omgeving, aan de hand van zogenaamde Release Notes met bijbehorende risicoanalyse, geïnformeerd wordt over deze wijzigingen. Op basis van deze Release Notes dient de Betaalvereniging te kunnen vaststellen dat het inderdaad een kleine wijziging betreft. In voorkomende gevallen kan de Betaalvereniging hierover in contact treden met de leverancier. De kleine wijzigingen zelf worden (inhoudelijk) achteraf door de Betaalvereniging getoetst. Deze toets vindt in ieder geval plaats binnen een periode van één jaar na aanmelding van de wijziging. Dit kan in de vorm van een aparte actie maar ook in combinatie met een grote wijziging in de security software.

Een uitzondering treedt op als de security software aantoonbaar voldoet aan PCI PTS 4.* én SRED - of recenter – in dat geval volstaat het om de Betaalvereniging te informeren over de doorgevoerde wijzingen. Met aantoonbaar wordt bedoelt dat de Betaalvereniging ten tijde van de initiële certificering heeft vastgesteld dat de betaalautomaat voldoet aan de EPC plus eisen, PCI PTS 4.* of recenter en dat ook de SRED module onderdeel is van de evaluatie waarvoor PCI het certificaat heeft afgegeven. Tevens moet de SRED module gebruikt worden voor de betaalketen waarover de Betaalvereniging geïnformeerd is.

De leverancier zal voor iedere gewijzigde security software versie (groot of klein) een conformiteitsverklaring (zie Bijlage 5) moeten afgeven waarin zij verklaart alleen security software operationeel in gebruik te nemen zoals gecertificeerd (in geval van grote wijzigingen) eventueel aangevuld met kleine wijzigingen zoals gemeld in de vorm van een Release Notes.

Daarnaast zal de leverancier voor iedere relevante wijziging in de betaalketen een conformiteitsverklaring (zie Bijlage 6) moeten afgeven waarin zij verklaart ten behoeve van de leden van de Betaalvereniging alleen gebruik te maken van deze betaalketen.

De wijze waarop dit onderzoek zal plaatsvinden is overeenkomstig de standaarden zoals opgenomen in Bijlage 2.

3.3 Beoordeling

De door het evaluatielaboratorium opgestelde onderzoeksrapporten zullen ter beschikking worden gesteld aan de Betaalvereniging. Hetzelfde geldt voor de evaluatie rapporten en andere getuigschriften waaruit blijkt dat de elementen uit de betaalketen voldoen aan relevante normen. De Betaalvereniging zal de rapporten beoordelen en toetsen aan de eisen zoals zijn beschreven in hoofdstuk 2.

Bij een akkoord (van het evaluatierapport) zal de Betaalvereniging de leverancier hierover schriftelijk informeren. Het bewijs van goedkeuring wordt verstrekt onder de voorwaarde dat er door de leverancier een conformiteitsverklaring wordt verstrekt. Door middel van deze verklaring staat de leverancier er voor in dat, voor security relevante componenten van, de betaalautomaat in gebruik wordt genomen in de operationele omgeving zoals beoordeeld. De conformiteitsverklaring moet zowel hardware, software aspecten van de betaalautomaat en achterliggende betaalketen afdekken (zie Bijlage 4, Bijlage 5 en Bijlage 6).

De in Bijlage 5 beschreven conformiteitsverklaring voor de software verwijst onder andere naar een door de Betaalvereniging vastgestelde methode om de authenticiteit van de software te waarborgen. In overleg is eventueel een andere, minimaal gelijkwaardige, methode ook toegestaan.
Daarnaast wordt de leverancier de mogelijkheid geboden om een Build&Sign procedure bij de Betaalvereniging uit te voeren. Voordeel van deze procedure is dat de leverancier gevrijwaard is van latere disputen over uitstaande software in het veld. Alleen door de Betaalvereniging getekende software kan in het veld uitstaan.

Bij een afwijzing (van het evaluatierapport) door de Betaalvereniging wordt de leverancier hierover schriftelijk en gemotiveerd geïnformeerd. Indien de leverancier niet akkoord wenst te gaan met deze afwijzing dan kan hij overeenkomstig artikel 8, lid 2 van de Overeenkomst betaalautomaatleverancier het geschil voorleggen aan het NAI.

In geval van een eventuele afwijzing bestaat er voor de leverancier de mogelijkheid om, na aanpassingen van de betaalautomaat resp. van het bijgestelde evaluatierapport, de betaalautomaat opnieuw aan te bieden bij de Betaalvereniging.

In bepaalde gevallen bestaat de mogelijkheid dat er ondanks dat er sprake is van een niet volledig geaccordeerd evaluatierapport door de Betaalvereniging onder voorwaarden een dispensatie wordt verstrekt. In geval het een dispensatie betreft die een relevante impact voor de acquirers kan hebben, zal de Werkgroep Beveiliging worden geconsulteerd. De Betaalvereniging behoudt de eindbevoegdheid om een dispensatie te verstrekken.

3.4 Toegestane verkoop - en gebruiksperiode van de betaalautomaat

De verkoopperiode wordt bepaald door de levensduur van het onderliggende PCI security certificaat. Voor SEPA zijn nog geen regels voor verkoopperiode afgesproken. Voor deze certificeringsprocedure wordt de PCI SSC regelgeving als uitgangspunt genomen. Dit betekent een mogelijk lange verkoopperiode van 10 jaar. Om de risico's hiervan te beperken wordt door de Betaalvereniging een aanvullende eis gesteld. Deze eis houdt in dat het security certificaat onderhouden dient te worden. Dit betekent dat de Betaalvereniging zich het recht voorbehoud om bijvoorbeeld naar aanleiding van nieuwe technologische ontwikkelingen een herbeoordeling uit te voeren. De herbeoordeling bestaat hieruit dat door de Betaalvereniging uitgaande van beschikbare evaluatierapporten (initiële en eventuele delta's) de betaalautomaat opnieuw evalueert ten opzichte van de op dat moment meest recente ontwikkelingen en aanvalstechnieken (door middel van desk-research). Op basis hiervan wordt door de Betaalvereniging, in overleg met de leverancier, bepaald of er nader onderzoek door het evaluatielaboratorium nodig is.

Wanneer in geval van nader onderzoek blijkt dat een betaalautomaat niet langer voldoet aan de normen beoordeelt de Betaalvereniging de impact van de afwijking en de evt. consequenties voor het security certificaat (bv. een eerdere expiratiedatum) in overleg met de terminalleverancier. Ook kunnen er . andere risico-beperkende maatregelen nodig zijn. Deze worden in overleg met de terminalleverancier vastgesteld.

De gebruiksperiode van de betaalautomaat (na datum einde security certificaat) wordt bepaald door regelgeving vanuit de card schemes. Als deze er niet is dan geldt dat een betaalautomaat maximaal vijf jaar na expiratie van het security certificaat in operationele omgeving gebruikt mag worden (zogenaamde 'sunset' regel van vijf jaar). In uitzonderingsgevallen, bij majeure security problemen, kan ook deze periode voor een bepaald type betaalautomaat worden verkort. In voorkomende gevallen zal de Betaalvereniging hierover in contact treden met betrokken marktpartijen.

Voor een nadere uitwerking van de PCI SSC-regelgeving naar onderliggende PCI standaard, in combinatie met de aanvullende maatregel van periodieke herbeoordeling wordt verwezen naar Bijlage 3.

3.5 Kosten en doorlooptijden

De totale doorlooptijd van de certificeringsprocedure door de Betaalvereniging is sterk afhankelijk van beschikbaarheid en kwaliteit van de opgeleverde rapporten. Gemiddeld bedraagt de doorlooptijd, vanaf het moment dat alle benodigde rapporten zijn aangeleverd bij de Betaalvereniging tot het geven van uitsluitsel over het wel/niet verstrekken van een bewijs van goedkeuring, twee weken.

De kosten voor alle onderzoeken van de betaalautomaat door evaluatielaboratoria, zoals geaccrediteerd door de Betaalvereniging, zijn voor rekening van de leverancier. De Betaalvereniging brengt de leverancier geen kosten in rekening voor het toekennen van bewijs van goedkeuring alsmede het publiceren daarvan op de website van de Betaalvereniging.

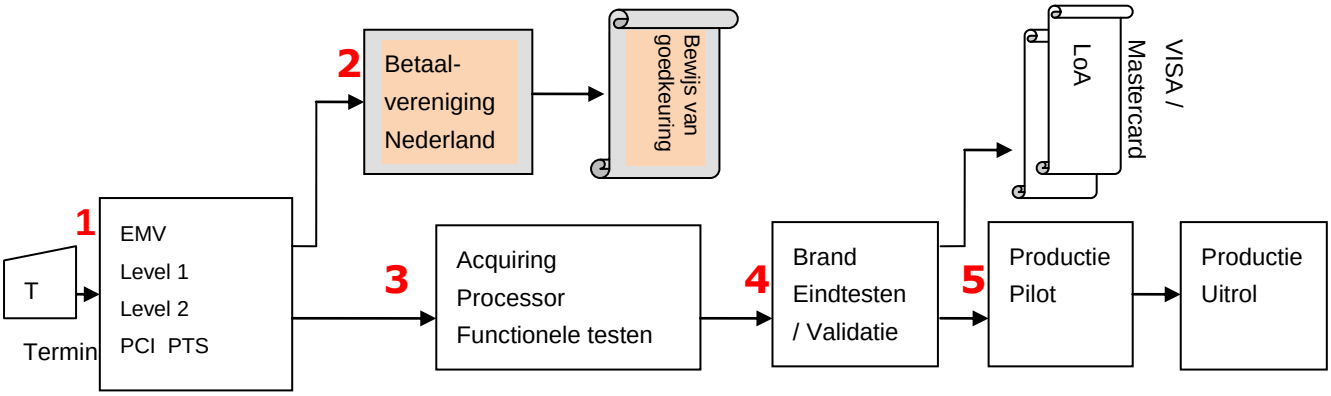
De kosten voor een herbeoordeling ten behoeve van onderhoud van het certificaat zijn voor rekening van de Betaalvereniging.

De kosten voor het beoordelen van het inbouw privacy shield zullen de eerste twee keer gedragen worden door de Betaalvereniging, met uitzonding van eventuele reis- en verblijfkosten die Betaalvereniging moet maken voor het beoordelen. Als aanwijzingen van de Betaalvereniging niet opgevolgd worden, zal de Betaalvereniging voor een derde beoordeling de gemaakte kosten in rekening brengen en daarbij uitgaan van 1250 euro exclusief BTW per werkdag.

Bijlage 1. Test- en Certificeringsmodel Betaalautomaten (INFORMATIEF)

In deze bijlage wordt aangeven hoe het totaalplaatje van certificering en toelating er uit ziet voor een Nederlandse betaalautomaat en de plek van het security certificaat van de Betaalvereniging daarin.

Schematisch:



De in onderhavig document bedoelde Procedure Security Certificering Betaalautomaten heeft uitsluitend betrekking op de hierboven genoemde Stap 2.

Stap 1

Deze stap omvat de door de global schemes voorgeschreven certificeringen:

- EMV level 1, voor de hardware certificering van de chipcard lezer
- EMV level 2, de software voor de chipcard afhandeling op de betaalautomaat
- PCI PTS, omvat o.a. de security eisen aan de betaalautomaat

Stap 2
In deze stap wordt op de aanwezigheid van bovengenoemde certificaten/goedkeuringen gecontroleerd. Deze certificaten dienen aan de Betaalvereniging overlegd te kunnen worden.

De security certificering van de Nederlandse betaalautomaat ziet er verder als volgt uit:

a. Een nadere evaluatie van de betaalautomaat door een erkend evaluatielaboratorium (zie Bijlage 10) tegen de normen zoals gepubliceerd in de meest recente EPC Volume (zie Bijlage 2).
   De evaluatie bestaat uit de volgende onderdelen:
   - Een hardware onderzoek (inclusief toetsing van Privacy Shield);
   - Een software onderzoek (code review) van de PED firmware
   - Een onderzoek naar de productie-procedures van de betaalautomaat, inclusief het initialiseren van de vendor keys;
   - Een onderzoek naar security services ten behoeve van een veilige afhandeling van de betaaltransactie door de betaalapplicatie, (bijv veilige communicatie naar de acquiring host)

b. De rapportage van het evaluatielaboratorium wordt door leverancier aangeboden aan de Betaalvereniging.

c. De Betaalvereniging beoordeelt de rapportage (kwaliteit, volledigheid, bevindingen, gemaakte afwegingen).

d. De Betaalvereniging verstrekt een bewijs van goedkeuring.

Het is, om redenen van efficiency qua tijd/kosten, aan te bevelen om gelijktijdig met PCI PED/PTS (zie stap 1) ook EPC PLUS te laten beoordelen.

Stap 3
De Acquiring Processor testen houden in:

a. Het functioneel testen van de betaalautomaat door een test laboratorium. (Voor CTAP zijn dit de zogenaamde FAT testen onder verantwoordelijkheid van Acquiris)

b. Het testen van de betaalautomaat tegen de host. (Voor CTAP zijn dit de zogenaamde NDT testen onder verantwoordelijkheid van de Acquiring Processor)

Stap 4

De EMV-productie testen op de Acquiring Host systemen omvatten:

a. MasterCard,Terminal Integration Proces (TIP)
b. VISA, Acquirer Device Validation Tool
c. Eventueel : End to End testen inclusief LB's (zoals 13.005_LB_bindend_Regelgeving-Uitbreiding-Brand-testen-v1-0)

Deze additionele eindtesten leiden bij Mastercard en VISA (global schemes) tot een certificaat voor de betaalautomaat om deze te mogen aansluiten aan het host systeem van desbetreffende Acquiring Processor.

Stap 5

Deze stap betreft de totale toetsing van de betaalautomaat:

a. Op de correcte werking aan de Acquiring productie Host (pilot)
b. Aan eventuele overige Acquiring Processor producten/diensten

Onder verantwoordelijkheid van de Acquiring Processor wordt in een pilot een beperkt aantal betaalautomaten nauwlettend gemonitored om te bezien hoe deze betaalautomaten in productie functioneren. Na een succesvolle afronding van de testen kan de Acquiring Processor besluiten de leverancier toestemming te geven de betaalautomaat aan te sluiten voor productie.

Voorwaarde voor deze procedure is de beschikbaarheid van certificaten/goedkeuringen zoals in Stap 1 verkregen. Deze certificaten/goedkeuringen dienen ter beschikking worden gesteld aan de Betaalvereniging.

Bijlage 2. Van toepassing zijnde eisen

Voor betaalautomaten die op de Nederlandse markt operationeel zijn gelden de Europese eisen zoals door de EPC gepubliceerd in haar Book4 van de SCS Volume v7.0. De laatste versie (7.0) van dit document is te vinden op: http://www.europeanpaymentscouncil.eu/index.cfm/sepa-vision-for-cards/sepa-cards-standardisation-volume-version-70-published-in-2014-ready-for-market-implementation/

De Europese eisen komen aanvullend op de eisen van de global schemes. Deze eisen zijn voor de global schemes opgesteld door PCI SSC. De volgende PCI standaarden zijn relevant:

- PCI PED 2.x, A (fysiek) , B (logisch) , C (online PIN) en D (offline PIN) requirements
- PCI PTS 3.x, A, B, C en D requirements (module CORE), E requirements (module Integration). Verder een module OP voor protectie van data over open, publieke (Internet en WiFi) verbindingen en een optionele module SRED voor protectie van kaarthouderdata (PAN).
- PCI PTS 4.x, zie PTS 3.x.

De volgende EPC PLUS eisen gelden voor de volgende PCI standaarden.

- PCI PED 2.x : privacy shield, code review PED firmware, productieprocedures, security services voor betaalapplicatie t.b.v. veilige betaaltransactie.
- PCI PTS 3.x: zelfde aanvullende eisen als voor PED 2.x
- PCI PTS 4.x: privacy shield, productieprocedures, security services voor betaalapplicatie t.b.v. veilige betaaltransactie.

PTS 4.x neemt de noodzaak weg voor de aanvullende eis van code review PED firmware.
PTS 3.x en PTS 4.x inclusief de modulen OP en SRED kunnen de betaalapplicatie ook de security services bieden voor de betaalapplicatie t.b.v. een veilige betaaltransactie.

De volgende publicaties zijn van belang voor een nadere toelichting (guidance) op de EPC PLUS requirements en de relatie met onderliggende PCI requirements.

- EPC343-08 Privacy Shielding for PIN Entry, version 1.4
- EPC plus POI DTR, versie 2.0 opgesteld door Betaalvereniging [update van CAS POI DTR versie 1.1.a, **momenteel onder revisie**].

PCI guidance is verkrijgbaar op de website van PCI SSC, zie:

- https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

EPC plus POI DTR guidance is verkrijgbaar bij de Betaalvereniging, zie Bijlage 10**.**

Bijlage 3. Levenscyclus certificaten

De toepasselijkheid van de PCI SSC-regelgeving in combinatie met de aanvullende eis (van periodieke herbeoordeling) heeft de onderstaande gevolgen. Hierbij wordt onderscheid gemaakt tussen de PCI+ betaalautomaten (de zgn. installed base) en nieuwe betaalautomaten.

Installed base automaten.
Voor bekende **PCI+ 1.3 terminals** zijn de regels als volgt:

1. PCI+ 1.3 betaalautomaten mogen niet meer verkocht en aangesloten worden op de betaalinfrastructuur.
2. Een onderhoudsperiode van vijf jaar is in werking getreden op 30 april 2014 voor de meeste van de PCI+ 1.3 terminals. Uitgezonderd een beperkt aantal automaten waarvoor de gebruiksperiode eerder dan in 2019 eindigt. Zie hiervoor de lijst van goedgekeurde automaten op de website van de Betaalvereniging.

Voor bekende **PCI+ 2.0 betaalautomaten** zijn de regels als volgt:

1. PCI+ 2.0 betaalautomaten mogen verkocht en aangesloten worden op de betaalinfrastructuur tot 30 april 2017, gelijk aan datum waarop PCI PED 2.x betaalautomaten nog uiterlijk verkocht en aangesloten mogen worden. De Betaalvereniging behoudt zich het recht voor om gedurende deze periode een herbeoordeling te initiëren (tegen PCI+ 2.0) wanneer daartoe aanleiding is. Daarna treed een onderhoudsperiode in werking.

Voor de **nieuwe betaalautomaten** geldt het volgende:

1. Nieuwe betaalautomaten dienen in bezit te zijn van een PCI PED 2.x, een PCI PTS 3.x of een PCI PTS 4.x certificaat. Ter aanvulling hierop dient de leverancier ook over een bewijs van goedkeuring van de Betaalvereniging te beschikken.
2. Voor betaalautomaten die gecertificeerd zijn tegen PCI PED 2.x geldt dat deze verkocht en aangesloten mogen worden op de betaalinfrastructuur tot 30 april 2017. De Betaalvereniging behoudt zich het recht voor om gedurende deze periode een herbeoordeling te initiëren wanneer daartoe aanleiding is. Hierna treedt een onderhoudsperiode in werking.
3. Voor betaalautomaten die gecertificeerd zijn tegen PCI PTS 3.x geldt dat deze verkocht en aangesloten mogen worden op de betaalinfrastructuur tot 30 april 2020. De Betaalvereniging behoudt zich het recht voor om gedurende deze periode een herbeoordeling te initiëren wanneer daartoe aanleiding is. , Hierna treedt een onderhoudsperiode in werking.
4. Voor betaalautomaten die gecertificeerd zijn tegen PCI PTS 4.x geldt dat deze verkocht en aangesloten mogen worden op de betaalinfrastructuur tot 30 april 2023.De Betaalvereniging behoudt zich het recht voor om gedurende deze periode een herbeoordeling te initiëren wanneer daartoe aanleiding is. Hierna treedt een onderhoudsperiode in werking.

Voor de onderhoudsperiode geldt generiek een periode van 5 jaar, tenzij anders bepaald door de card schemes welke op de betaalautomaat geaccepteerd worden[1]. Zie ook de lijst van goedgekeurde automaten op de website van de Betaalvereniging waar de onderhoudstermijnen gepubliceerd staan.

[1] Zo heeft VISA in een eerder stadium onderhoudstermijnen gesteld voor PCI 1.x gecertificeerde betaalautomaten. En daarbij het voornemen geuit om dat ook voor de PCI 2.x gecertificeerde betaalautomaten te gaan doen.

Bijlage 4. Sjabloon Conformiteitsverklaring voor hardware POI

Ondergetekende,

De <firmanaam>, gevestigd te <postcode>, <plaats>, <bezoekadres>,
te dezen rechtsgeldig vertegenwoordigd door <naam>,
hierna te noemen: Leverancier

Overwegende:

- dat Leverancier op ….de Standaardovereenkomst betaalautomaatleverancier met de Betaalvereniging heeft ondertekend;
- dat …. [hier doel van deze verklaring invullen ..]

Verklaart in aanvulling op de Standaardovereenkomst betaalautomaatleverancier het volgende:

1. Leverancier zal ten behoeve van de Acquirers, zijnde leden van de Betaalvereniging Nederland (hierna: de Betaalvereniging) slechts betaalautomaten met een bewijs van goedkeuring van de Betaalvereniging leveren in overeenstemming met het type zoals door hem aangeboden ter certificering. Als referentie-exemplaar is de betaalautomaat met serienummer <> aangeboden aan de Betaalvereniging.
2. Leverancier stemt er mee in dat het aangeboden referentie-exemplaar in bewaring blijft bij de Betaalvereniging zolang de betaalautomaat actief deelneemt in het betalingsverkeer. Het referentie-exemplaar blijft eigendom van de Leverancier.
3. Leverancier draagt de verantwoordelijkheid voor de componenten die hij inkoopt van derden. Om deze verantwoordelijkheid te kunnen dragen heeft de Leverancier overeenkomsten gesloten met zijn toeleveranciers of met de partijen waarvan hij inkoopt.
4. Veranderingen aan de betaalautomaat of in het productieproces van de betaalautomaat - in relatie tot de geldende beveiligingseisen - zullen tijdig ter beoordeling voorgelegd worden aan de Betaalvereniging. Niet eerder dan na schriftelijke goedkeuring door de Betaalvereniging zullen de wijziging(en) conform het voorgelegde verzoek worden doorgevoerd.
5. Schade die voortvloeit uit het niet nakomen van deze Conformiteitsverklaring is voor rekening van de Leverancier.

Plaats …… datum ……

Voor < Leverancier >

Naam:
Titel:

Bijlage 5. Sjabloon Conformiteitsverklaring voor software POI

Ondergetekende,

De <firmanaam>, gevestigd te <postcode>, <plaats>, <bezoekadres>,
te dezen rechtsgeldig vertegenwoordigd door <naam>,
hierna te noemen: Leverancier

Overwegende:

- dat Leverancier op ….de Standaardovereenkomst betaalautomaatleverancier heeft ondertekend;
- dat …. [hier doel van deze verklaring invullen ..]

Verklaart in aanvulling op de Standaardovereenkomst betaalautomaatleverancier het volgende:

1. Leverancier zal ten behoeve van de Acquirers, zijnde leden van Betaalvereniging Nederland (hierna: de Betaalvereniging) slechts door de Betaalvereniging gecertificeerde - of in het geval van een kleine wijziging nog te certificeren - security software leveren. Indien de gecertificeerde security software voorziet in SRED, dan moeten deze software uitgerold worden.
2. De meest recente gecertificeerde security software versie heeft de volgende kenmerken:
   - Gegevens van het evaluatierapport: <Titel, versie, datum E-lab>
   - <Sha-1|Sha-2> HASH berekend over de broncode zoals vermeld in het evaluatie rapport.
   - Beschrijving van Build environment:
     - Besturingssysteem, Service Pack| Patch niveau e.d.;
     - Leverancier, versienummers e.d. Build environment compiler e.d. (voldoende informatie om vanaf beginsituatie Build environment op te kunnen bouwen);
   - <Sha-1|Sha-2> HASH berekend over resulterende binary c.q. compilatie resultaat.
3. Alleen van toepassing indien er kleine wijzigingen zijn:
   - Gegevens van release note: <Titel, versie, datum>
   - Risicoanalyse, zelf uit te voeren ter onderbouwing van/behorende bij wijziging, § release note of separaat document.
   - <Sha-1|Sha-2> HASH berekend over de broncode zoals vermeld in release note.
   - Optioneel als deze gelijk is aan punt 2
     [Beschrijving van Build environment:]
     - Besturingssysteem, Service Pack /| Patch niveau e.d.
     - Leverancier, versienummers e.d. Build environment compiler e.d.
     - E.d. (voldoende informatie om vanaf beginsituatie Build environment op te kunnen bouwen)
   - <Sha-1|Sha-2> HASH berekend over resulterende binary c.q. compilatie resultaat.

4. Leverancier stemt er mee in dat de broncode in bewaring blijft bij de Betaalvereniging of een door haar aangewezen externe partij (escrow, evaluatielaboratorium) zolang de betaalautomaatsoftware actief deelneemt in het betalingsverkeer. De broncode blijft eigendom van de leverancier.
5. Leverancier draagt verantwoordelijkheid voor het beschikbaar blijven van de componenten die nodig zijn om van gecertificeerde broncode te komen tot de vastgelegde binary c.q. compilatie resultaten.
6. Veranderingen aan de security software - in relatie tot de geldende beveiligingseisen - zullen tijdig ter beoordeling voorgelegd worden aan de Betaalvereniging.
7. Grote wijzigingen zullen niet eerder dan na schriftelijke goedkeuring van de security software door de Betaalvereniging worden doorgevoerd.
8. Kleine wijzigingen kunnen na het informeren van de Betaalvereniging, aan de hand van Release Notes, worden doorgevoerd (maximaal binnen één jaar alsnog certificering).
9. Schade die voortvloeit uit het niet nakomen van deze Conformiteitsverklaring is voor rekening van de Leverancier.

Plaats …… datum ……

Voor < Leverancier >

Naam:
Titel:

Bijlage 6. Sjabloon Conformiteitsverklaring Betaalketen voor <POI>

Ondergetekende,
Ondergetekende,

De <firmanaam>, gevestigd te <postcode>, <plaats>, <bezoekadres>,
te dezen rechtsgeldig vertegenwoordigd door <naam>,
hierna te noemen: Leverancier

Overwegende:

- dat Leverancier op ….de Standaardovereenkomst betaalautomaatleverancier heeft ondertekend;
- dat …. [hier doel van deze verklaring invullen ..]

Verklaart in aanvulling op de Standaardovereenkomst betaalautomaatleverancier het volgende:

1. Leverancier zal ten behoeve van de Acquirers, zijnde leden van Betaalvereniging Nederland (hierna: de Betaalvereniging) slechts door de Betaalvereniging gecertificeerde betaalautomaten aansluiten aan de hieronder beschreven betaalketen.
2. De betaalketen - van betaalautomaat tot aan de transactie verwerkende systemen van de acquirer processor die door een of meerdere de Acquirers van Betaalvereniging Nederland gebruikt worden - is opgebouwd uit de volgende elementen (Het gaat hier om die elementen variërend van kaartlezer tot en met servers waar toegang verkregen kan worden tot gevoelige kaartdata en/of sleutelmateriaal waarmee de kaartdata en/of pincode beveiligd is):
   i) <EPP|PED>
   ii) [Kaartlezer, igv onbemande betaalautomaten]
   iii) [Concentrator/Front-end processor]
   iv) [HSM]
   v) Acquirer processor

<gelieve een figuur op te nemen die de keten schetst>

3. Onder punt 2 genoemde keten elementen voldoen aan de volgende beveiligingsstandaarden: <PCI PTS, PCI DSS, PCI PA-DSS, PCI HSM, PCI PIN> (per keten element specificeren)

4. Tussen de - onder punt 2 genoemde – keten elementen wordt gebruik gemaakt van de volgende Point-to-Point encryptie methode:
   <Bijvoorbeeld: De betaalketen van 2i tot en met 2v gebruikt SRED en S-UKPT volgens de C-Tap 10 specificaties
   - of –
   De betaalketen van 2i tot en met 2ii gebruikt SRED; van 2i tot en met 2ii wordt gebruik gemaakt van Three-key Triple DES DUKPT; van 2ii tot en met 2v wordt gebruik gemaakt van S-UKPT volgens de C-Tap 3specificaties>
5. Veranderingen aan de betaalketen - in relatie tot de geldende beveiligingseisen - zullen tijdig ter beoordeling voorgelegd worden aan de Betaalvereniging.
6. Schade die voortvloeit uit het niet nakomen van deze Conformiteitsverklaring is voor rekening van de Leverancier.

Plaats …… datum ……

Voor < Leverancier >

Naam:
Titel:

Bijlage 7. Certificeren van non-pincode betaalautomaten

1. Algemeen

De security certificering van betaalautomaten is voor een belangrijk deel gericht op de security module die noodzakelijk is bij gebruik van een pincode als authenticatiemiddel voor een elektronische betaaltransactie.
Marktontwikkelingen hebben er voor gezorgd dat ook betaalautomaten zonder ondersteuning van pincode invoer beschikbaar zullen komen. De regelgeving van de Global Brands staat dit toe. Omdat deze betaalautomaten een ander (security) risico profiel hebben, zal voor deze non-pincode betaalautomaten een afwijkende certificeringsprocedure worden gehanteerd.

2. Eisen

Er is een een secure protocol vereist bij de communicatie tussen de acquiring host en de betaalautomaat bij non-pin automaten. Het secure protocol dient wederzijdse authenticatie en beveiligde berichtenuitwisseling tussen betaalautomaat en host te waarborgen. Dit veronderstelt ook een integere betaalapplicatie. Het is aan de acquirer (processor) om het security protocol te specificeren en in te regelen.

Het is vervolgens aan de leverancier van de betaalautomaat om het security protocol te ondersteunen op een veilige wijze. Zo mogen geheime sleutels (naar algemeen geaccepteerde ISO-beveiligingsstandaarden) bijvoorbeeld niet in klare waarde voorkomen in onbeschermd geheugen van de betaalautomaat.

De van toepassing zijnde internationale eisen staan opgenomen in de SEPA Cards Standardisation Volume version 7.0. Naast de SRED verplichting gelden de volgende eisen: I2, I3, I4, K9 en K17.

3. Procedure

(a) registratie

Om zicht te houden op de uitrol van non-pincode betaalautomaten dient de leverancier van de betaalautomaat zich te registreren (inclusief het sluiten van een Overeenkomst) bij de Betaalvereniging onder aangeving van welke security en functionele certificeringen de betaalautomaat doorlopen heeft.

(b) beoordeling

In geval van een CTAP TSC gecertificeerde betaalautomaat kan worden aangenomen dat de betaalautomaat beveiligde communicatie (inclusief wederzijdse authenticatie) met de acquiring host op een veilige wijze ondersteunt. In geval van andere betaalautomaten (bijv. IFSF, CTAP SSL3/TLS-only) moet dit blijken uit een vorm van (acquiring) certificering. Bij het ontbreken van een CTAP TSC certificaat is het aan de leverancier om aan te tonen dat de betaalautomaat het voorgeschreven security protocol op veilige wijze heeft geïmplementeerd. Voor deze categorie van betaalautomaten mag dit aangetoond worden aan de hand van ontwerp- (en test)documentatie. De documentatie wordt beoordeeld door de Betaalvereniging. Mocht daar aanleiding voor zijn, dan behoudt de

Betaalvereniging zich het recht voor de documentatie te laten valideren door een extern lab. Als onvoldoende blijkt dat de betaalautomaat op een veilige wijze het security protocol ondersteunt en er risico's zijn, wordt dit gesignaleerd richting acquirer. De Betaalvereniging zal, in overleg met betrokken acquirer, vast stellen welke risico beperkende maatregelen genomen kunnen worden om de veiligheid voldoende te kunnen garanderen voor de betaalketen.

(c) Levenscyclus en bewijs van goedkeuring

De leverancier tenslotte ontvangt van de Betaalvereniging een toelatingsbrief waarin de goedkeuringstermijn is aangegeven. Deze termijn zal gelijk zijn aan de betaalautomaten met pincode gebruik, waarbij de periodieke herbeoordeling komt te vervallen.

Bijlage 8. Procedure beoordelen Privacy Shield

Als een betaalautomaat geïntegreerd wordt in een ‘vending machine’ dan moet voldaan worden aan “EPC343-08 PRIVACY SHIELDING FOR PIN ENTRY” Versie 1.4 van 30 September 2009.

Deze beoordeling kan uitgevoerd worden door een van de erkende laboratoria of door de Betaalvereniging. Deze beoordeling kan uitgevoerd worden door het opnemen van de maatvoering aan de hand van een eerste referentie exemplaar. Ook kan gebruik worden gemaakt van technische tekeningen zodat aan de hand van maatvoering bepaald kan worden of aan de norm voldaan is. De toets-5 is het referentie punt om de hoogte van het privacy shield te bepalen maar ook voor het bepalen van de inbouw hoogte, gerekend vanaf de grond tot het midden van toets-5. Daarvoor ontvangen wij graag maatgegevens van het inbouwframe in combinatie met de gecertificeerde betaalautomaat (bij voorkeur CAD tekeningen in PDF formaat) en de ‘vending machine’.

Bij een akkoord zal de Betaalvereniging de leverancier hierover schriftelijk informeren. Het bewijs van goedkeuring wordt verstrekt onder de voorwaarde dat er door de leverancier een conformiteitsverklaring wordt verstrekt. Door middel van deze verklaring staat de leverancier er voor in dat, voor security relevante componenten van, de betaalautomaat in gebruik wordt genomen in de operationele omgeving zoals beoordeeld. De conformiteitsverklaring moet zowel hardware als plaatsingsaspecten afdekken (zie Bijlage 9).

Bijlage 9. Conformiteitsverklaring Inbouwmethode <POI>

Ondergetekende,

De <firmanaam>, gevestigd te <postcode>, <plaats>, <bezoekadres>,

te dezen rechtsgeldig vertegenwoordigd door <naam>,

hierna te noemen: Automaatleverancier

Verklaart het volgende:

1. Automaatleverancier zal ten behoeve van toepassing voor de Nederlandse markt conform de norm:
   - EPC343-08 Version 1.4 approved 30 September 2009, PRIVACY SHIELDING FOR PIN ENTRY

   beoordeelde <typenaam van automaat> leveren zoals door hem aangeboden ter beoordeling <referentie naar tekening met maatvoering>.

2. Veranderingen aan de <typenaam van automaat> die van invloed zijn op de richtlijnen zoals verwoord in de *norm* zullen tijdig ter beoordeling voorgelegd worden aan de Betaalvereniging Nederland. Niet eerder dan na schriftelijke goedkeuring door de Betaalvereniging Nederland zullen conform het voorgelegde verzoek de wijziging(en) worden doorgevoerd.

3. Schade die voortkomt uit het niet nakomen van deze Conformiteitsverklaring is voor rekening van de Automaatleverancier.

Plaats …… datum ……

Voor < Automaatleverancier >

Naam:

Titel:

Bijlage 10. Contactgegevens

Aanmeldingen

Betaalvereniging Nederland

Bezoekadres: Beethovenstraat 300 , 1077 WZ Amsterdam
Postadres:Postbus 83073, 1080 AB Amsterdam

Contactpersonen: dhr. O. Covers, dhr. R. Steenbeeke.

Telefoon: +31 20 305 1900
Fax: +31 20 305 1912
E-mail: o.covers@betaalvereniging.nl, r.steenbeeke@betaalvereniging.nl
website: www.betaalvereniging.nl

Geaccrediteerde evaluatielaboratoria
De Betaalvereniging accepteert onderzoeken van o.a. de volgende onderzoeksinstituten:

Brightsight BV
Delftechpark 1
2628 XJ Delft

Telefoon: +31 (0)15 2692500
Fax: +31 (0)15 2692555
E-mail: marrewijk@itsef.com
Website: www.brightsight.com

T-Systems GEI GmbH
Vorgebirgsstrasse 49,
D-53119 Bonn
Duitsland

Telefoon: +49 228 9841 114
Fax: +49 228 9841 60
E-mail: robert.hammelrath@t-systems.com
Website: http://www.t-systems.de/ict-security

Security Research & Consulting GmbH
Graurheindorfer Strasse 149a
53117 Bonn
Duitsland

Telefoon:+49 2282806101
E-mail: detlef.kraus@src-gmbh.de
Website: www.src-gmbh.de

TÜV Informationstechnik GmbH
PO Box 103261
45032 ESSEN
Mr F. Beuting

Bijlage 11. Verklarende woordenlijst

ATM	Automated Teller Machine
BEA	BetaalAutomaat
CIM	Contract Information Manager, het systeem waarin de verwerkingscontacten worden bewaard. Het gaat met name om de technische parameters die voortkomen uit het Contract tussen Acceptant en Acquirer die per terminal en per brand worden vastgelegd.
CTAP	Common Terminal Acquirer Protocol. CTAP is een multi host multi acquirer betaalinfrastructuur en architectuur voor het verwerken van Point of Sale transacties.
Debit	De methode van elektronisch betalen waarbij het te betalen bedrag onmiddellijk van de rekening van de pashouder wordt afgeschreven. In de context van deze risicoanalyse wordt hiermee het betalen met magneetstrip plus PINcode (“PIN” in de volksmond) bedoeld.
ECB	European Central Bank
EPC	European Payment Council- werd opgericht in 2002. Het noemt zichzelf "het besluitvormend en coördinatieorgaan van de Europese banksector met betrekking tot betalingen". De belangrijkste taak van de EPC is de ontwikkeling van de Single Euro Payment Area. De 74 leden zijn banken en verenigingen van banken.
EMV	Europay, MasterCard en Visa, ontwikkelaars en eigenaar van het protocol.
GEA	GEldAutomaat
IFSF	International Forecourt Standards Forum – is een Europese organisatie die standaarden ontwikkeld voor het aansluiten van apparaten op een tankstation, zoals dispensers, Tank Level Meters, Prijzenborden, autowasstraten en Outdoor betaalterminals. Niet alleen betaalautomaten in de Pertol branche maken gebruik kan IFSF, IFSF wordt ook gebruikt door terminalleveranciers voor bijvoorbeeld parkeeroplossingen maar ook voor postagentschappen.
LoA	Letter of Approval, goedkeuringsbrief
Maestro	Product van MasterCard voor acceptantbetalingen met debitcard.
NAI	Nederlands Arbitrage Instituut – voor behandeling geschillen met betrekking tot de beoordeling van een betaalautomaat door de Betaalvereniging Nederland.
Onbemande betaalautomaat	De kaarthouder verricht de transactie volledig zelfstandig, zonder tussenkomst van een kassière. Voorbeelden zijn betaalautomaten geïntegreerd in: Vending Machine, kaartverkoop machine, zelf service zuil e.d.
PAN	Primary Account Number. 14 of 16-cijferige numerieke code gecodeerd in de EMV-chip en op de magneetstrip (bij Credit Card embossed op de voorzijde). De PAN is een samengesteld getal, waarvan de eerste 6 het Issuer Identification Number (IIN) zijn van de kaartuitgever. Het eerste cijfer van de IIN is de Major Industry Identifier (bankpassen beginnen daarom altijd met 3, 4, 5, of 6). Hierna volgt het individuele kaartnummer van de kaarthouder, alsmede een controlecijfer of code die de authenticiteit van de PAN controleert.

PCI	Payment Card Industry
PCI-EPP	Payment Card Industry – Encrypting Pin Pad (standaard)
PCI-PTS	Payment Card Industry – PIN Transaction Security (standard). Voor PCI versie 1.3 en 2.1 de verzamelnaam voor de verschillende PCI programma's als EPP, PED, UPT en HSM. PCI PTS versie 3 heeft het over een Point Of Interaction (POI) om eerder genoemde architecturen te beschrijven.
PIN	Persoonlijk Identificatie Nummer. Gangbare term voor het betalen met debit.
POI	Point of Interaction
POS	Point Of Sale
SRED	Secure Reading and Exchange of Data - is onderdeel van de PCI PTS standard om gelezen kaartdata direct na het lezen ervan te beschermen c.q. te vercijferen
TMS	Terminal Management Systeem
TSC	Terminal Secure Component. - TSC Certificaat – het TSC Certificaat is uniek en wordt gebruikt voor de sleutelrelatie tussen betaalautomaat en transactie verwerkende host. Een certificaat bindt een publieke sleutel aan een bepaalde unieke naam.
V PAY	Product van Visa voor acceptantbetalingen met debitcard