VALITOR

Business beyond borders

Öryggisupplýsingar

Ingenico posar

Útgáfa IPA 1.6.X

Version 1.1.1 22.05.2014

FILE HISTORY

Date	Author(s)	Version Description
24.5.2012	Sigmar Jónsson, Þórhildur Baldursdóttir og Tara Kathleen Flynn	Útgáfa 1.0.1 Fyrsta útgáfa að skjalinu
23.5.2013	Sigmar Jónsson, Þórhildur Baldursdóttir og Þórður Ingi Guðmundsson	Útgáfa 1.1.0 GPRS/3G netstillingum bætt við
22.5.2014	Sigmar Jónsson	Útgáfa 1.1.1 Uppfærsla vegna útgáfu 1.6.8

1 ÖRYGGISUPPLÝSINGAR

1.1 PA-DSS VOTTUN

Útgáfa IPA 1.6.X af greiðsluhugbúnaðinum er PA-DSS vottaður fyrir Ingenico iCT2XX and IWL2XX posa.

Til að staðfesta að hugbúnaðurinn í posanum sem þú notar sé PA-DSS vottaður. Ýtið á F – Payment - Útgáfa. Posinn mun núna sýna útgáfunúmer hugbúnaðar. Nafn posa og útgáfa hugbúnaðarins ætti að vera listað saman á eftirfarandi vefsíðu undir nafni VALITOR:

https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

1.2 PA-DSS STILLING

Seljandi getur ekki breytt stillingum tengdum öryggi kortaupplýinga í posa-hugbúnaðinum. Öllum stillingum er stjórnað af þjónustuaðila.

1.3 ÖRYGGISUPPLÝSINGAR

- ✓ Fullt kortnúmer er prentað á kvittun seljanda. Fullt kortnúmer á nótu krefst þess að seljandi meðhöndli kvittanir eftir öryggisstöðum PCI. Sjá nánar á www.pcisecuritystandards.org (PA-DSS 2.1)
- ✓ Söluaðila ber að geyma söluaðilanótur í samræmi við skilmála viðkomandi færsluhirðis
- ✓ Dulkóðaðar kortaupplýsingar eru geymdar í posanum, þangað til bunki er sendur. Mælt er með að bunki sé sendur í lok hvers dags. Posinn tekur ekki við nýjum færslum ef færslur í honum eru fimm daga gamlar eða eldri. Áður en posa er skilað aftur til þjónustuaðila skal senda inn bunkann. (PA-DSS 2.1)
- ✓ Samskipti eiga sér stað yfir IP-net, IP-net yfir bluetooth eða GPRS/3G. Það eru engin skilyrði sett um eldvegg á netkerfi söluaðila. IP og IP yfir bluetooth tengdur posi stofnar net tengingar frá neti söluaðila á eftirfarandi portum: (PA-DSS 5.4)
    - Port 443 til að eiga samskipti vegna heimildagjafar og bunka innsendingar yfir SSL
    - Port 6000 til að sækja uppfærslur til þjónustuaðila.

  Allir nauðsynlegir íhlutir fyrir samskipti eru afhentir með posanum og er ekki mögulegt fyrir söluaðila að breyta því.

1.4 ÝTARLEGRI ÖRYGGISUPPLÝSINGAR

- ✓ Posa hugbúnaðurinn geymir engar viðkvæmar kortaupplýsingar eins og segulrönd, PIN eða öryggiskóða kortsins. Allar upplýsingar úr fyrri útgáfum hugbúnaðarins hafa verið fjarlægðir af posanum af þjónustuaðila (PA-DSS 1.1.4, 1.1.5)
- ✓ Kortaupplýsingar eru geymdar á tveim mismunandi stöðum í posanum:
  - traECBPan og traECBExpDat geymir dulkóðaðar kortaupplýsingar frá bunkanum
  -traHashPan geymir einstefnu dulkóðun (hash) yfir 10 síðustu kortnúmer sem hefur verið synjað um heimild. Gögnin eru geymd í Flash minni. Skráin er einnig notuð til að bera saman kortið sem notað var í síðustu aðgerð við þá aðgerð sem er í gangi. (PA-DSS 2.1)

- ✓ Nýr dulkóðunarlykkill er stofnaður inn í posanum þegar fyrsta færslan er vistuð í tækinu. Dulkóðunarlykillinn er hreinsaður eftir að bunki hefur sendur eða hreinsaður. Dulkóðunarlyklar eru ekki aðgengilegir frá posa hugbúnaðinum. (PA-DSS 2.5 – 2.7)
- ✓ Posa hugbúnaðurinn hefur ekkert viðmót svo að söluaðili geti fengið aðgang að kortagögnum og er því engin aðgangsstjórnun eða skráningarsaga nauðsynleg. (PA-DSS 3,1, 3,2, 4,1, 4,4)
- ✓ Posinn getur aðeins átt samskipti í gegnum net snúru, bluetooth eða GPRS/3G en ekki í gegnum þráðlaust net. (PA-DSS 6.1, 6.2)
- ✓ Posinn er eina tækið sem geymir greiðslukortaupplýsingar og eru þær ekki sendar á önnur kerfi hjá söluaðila. (PA-DSS 9.1)
- ✓ Ekki er hægt að stofna fjarlæg samskipti við posann. Posinn á samskipti við sinn þjónustuaðila á 14 daga fresti til að athuga með mögulegar uppfærslur á stillingum og hugbúnaði. (PA-DSS 10.2, 10.3.1, 10.3.2)
- ✓ Posinn notar SSL til að verja kortaupplýsingar við flutning. Söluaðili hefur engan aðgang að öryggis stillingum (PA-DSS 11.1, 11.2)
- ✓ Posa hugbúnaðurinn gefur ekki kost á “non-console” stjórnunar aðgang. (PA-DSS 12.1)