

Report from review of kiosk for Megatec, IS650

Participants:

Stefan Lund, SecureCom and PNC SAC.

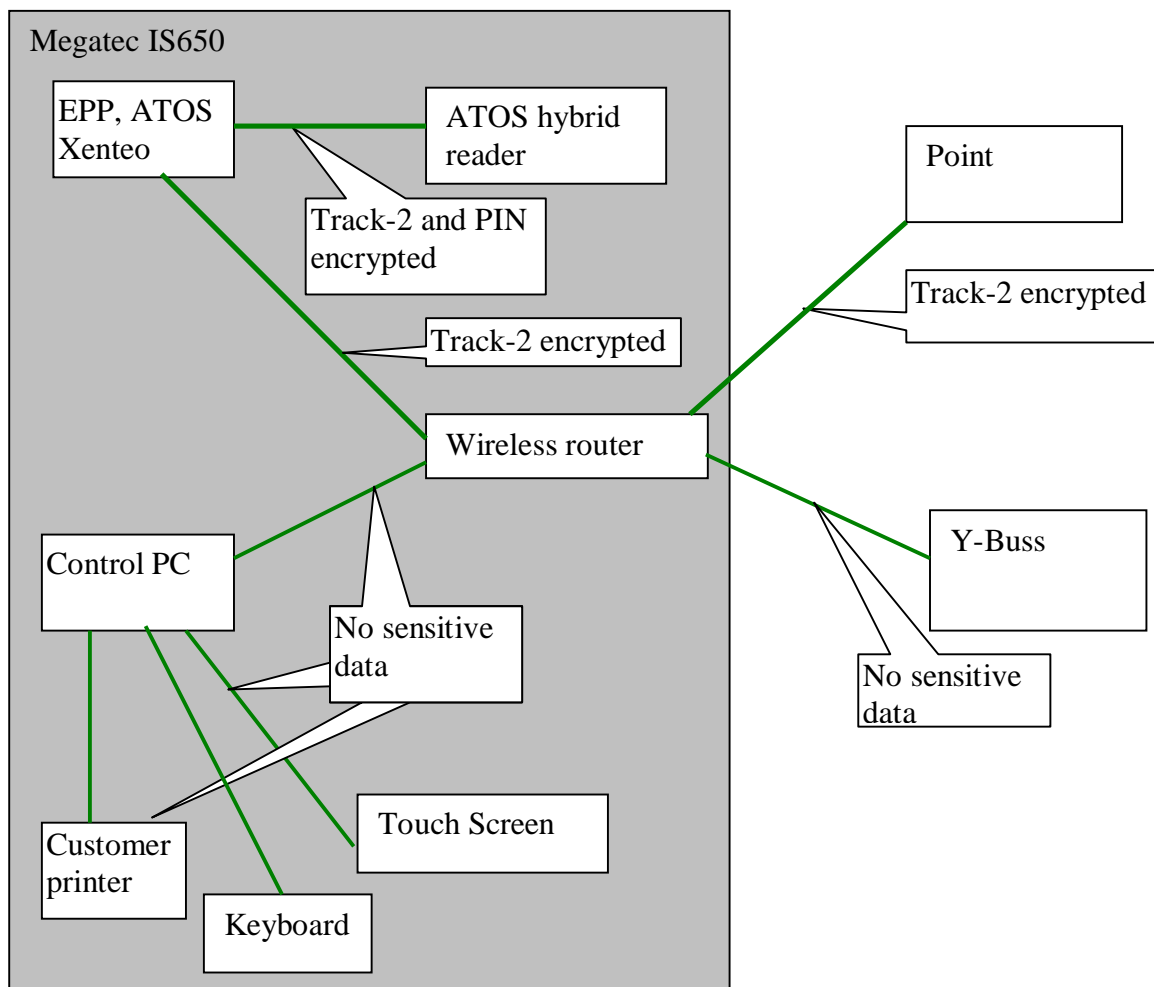
Hans Axelsson, Megatech

System overview

The kiosk is hereafter called UPT (Unattended Payment Terminal) .

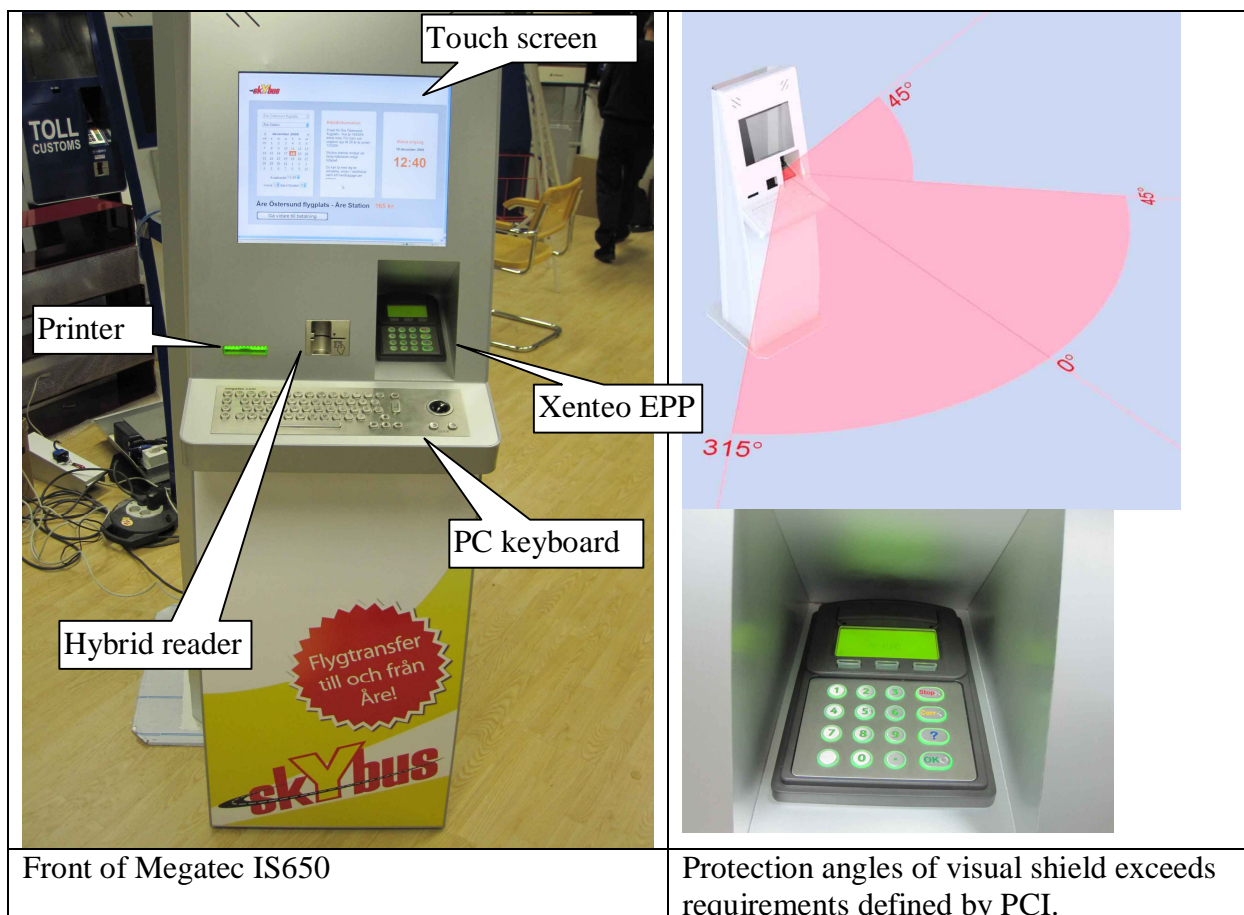
The UPT consists of the following main components:

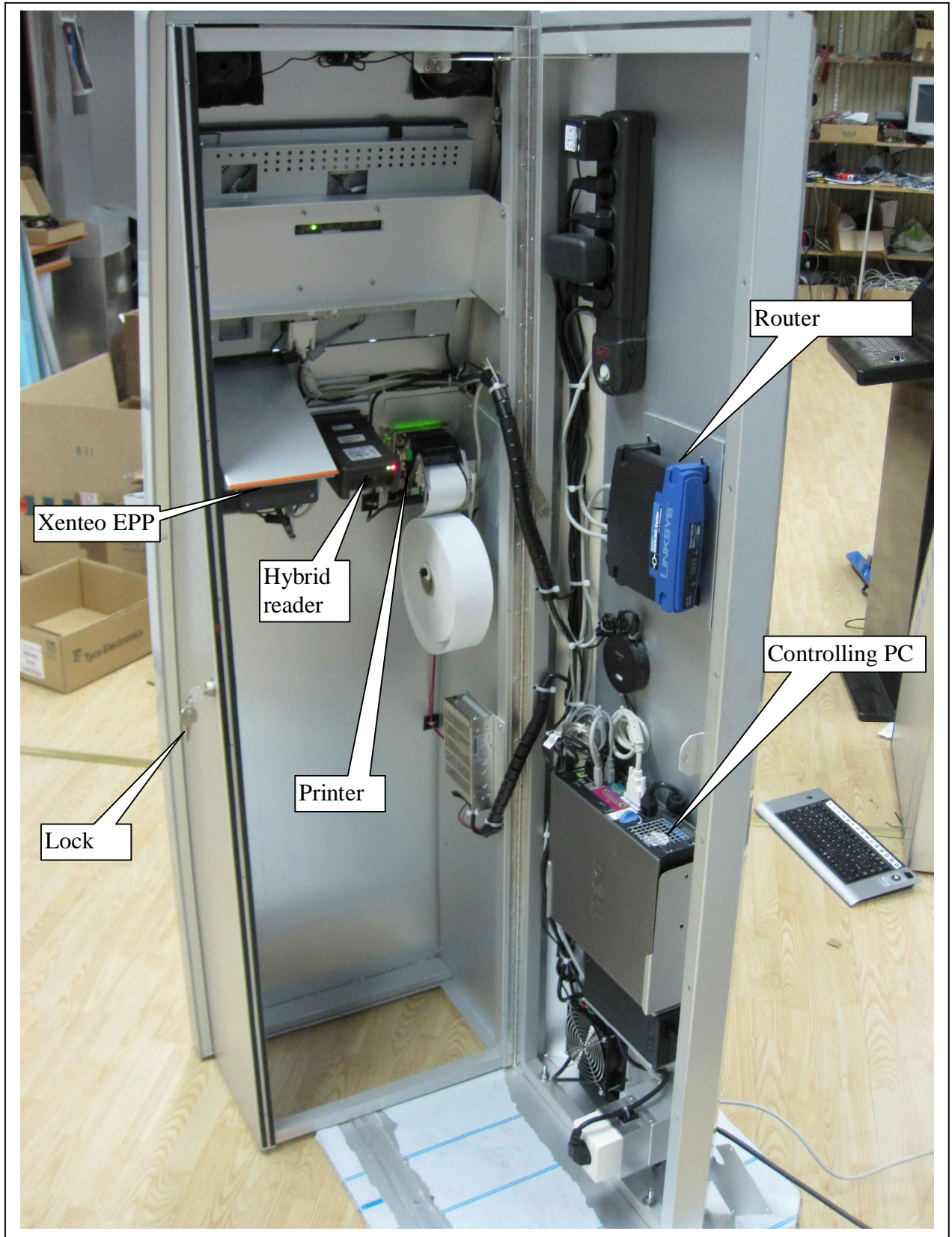
- A PED, Atos Xento
- Atos Hybrid reader
- A control PC
- A touch screen
- A cabinet consisting of sheet metal.
- A printer for the customer receipt/bus ticket
- A full size PC keyboard with a built in mouse (roll mouse?)



Summary of security features

- Track-2 and PIN are encrypted between reader and EPP. Encryption was reviewed by PNC SAC when Xenteo was approved together with hybrid reader.
- Sensitive data is line encrypted between Xenteo EPP and Point using SSL where sender and receiver are verified using certificate. (Certificate will prevent man in the middle attack)
- Sensitive data is not handled by control PC or printed by printer.
- Communication between Point and the buss is wireless (3G communication).
- The touch screen will not support any numeric input. Xenteo will not support numeric input except PIN.
- The PC keyboard can be used for numeric input.
- The cabinet have 1 lock.
- The cabinet does not have an alarm.
- The application running in the PC is protected from unauthorized update by "SiteKiosk", <http://www.sitekiosk.com/en-US/SiteKiosk/Default.aspx>
- The application running in the PC is browser displaying both internal and external (WEB) pages.





Inside of Megatec IS650

Reflections regarding security

It will not be possible to eavesdrop any communication inside the cabinet since all sensitive data is encrypted by Secure Devices.

One attack scenario is to mount a camera above the PIN keyboard and then also add a magtrack skimmer that is mounted outside of the original magtrack reader. To prevent this the following actions can be done:

- Daily external inspections of UPT is required
- Show a picture of how the front of the UPT should look like to the card holder, e.g. when instructing the cardholder to enter PIN/insert card

If the application in the controlling PC is modified by a fraudster then the fraudster may tell the card holder to enter PIN on the PC keyboard instead of the EPP, then PIN can be read in plain text by the modified terminal software. To protect against this attack:

- Only software approved by authorized personal may execute in the controlling PC, this might be done by "SiteKiosk"
- Daily external inspections could include to make a fake transaction to see if the cardholder is instructed to enter PIN on the EPP or the PC keyboard.
- This will with high probability be detected by the card holder since there is an Xenteo EPP available. Possibly the keyboard might be considered to be the same as used by SJ where PIN entry is done on a similar keyboard, however to succeed with this attack the fraudster not only have to modify the application the fraudster must also hide/cover the EPP.

The most (only) likely attack scenario is shoulder surfing. After the PIN has been observed by the fraudster, the fraudster steals the original card from the cardholder. To make shoulder surfing attack more difficult the following actions can be taken:

- Recommend cardholder to cover PIN entry with other hand.
- A high visual shield.
- Location or orientation of Kiosk should make it difficult to stand close behind of the cardholder undetected (not possible in this environment?)
- Remind cardholder to remove card from card reader after EMV transaction is finished. If possible do not print Bus ticket before card is removed.

Actions needed

Documented routines are needed regarding:

- Daily external inspections. This should include a description of
 - What to look for. (Cameras, additions to card reader, if the cabinet is broken). Should include photos of how the kiosk should look when it is not modified. The inspector should also look for cameras or mirrors directed towards the keyboard.
 - Routines on what to do if a modification of the Kiosk is detected.
- Routine for installation and transport of sensitive components (Hybrid Reader and EPP)
- Routine for replacing EPP or Hybrid reader. Must be done by authorized personal.