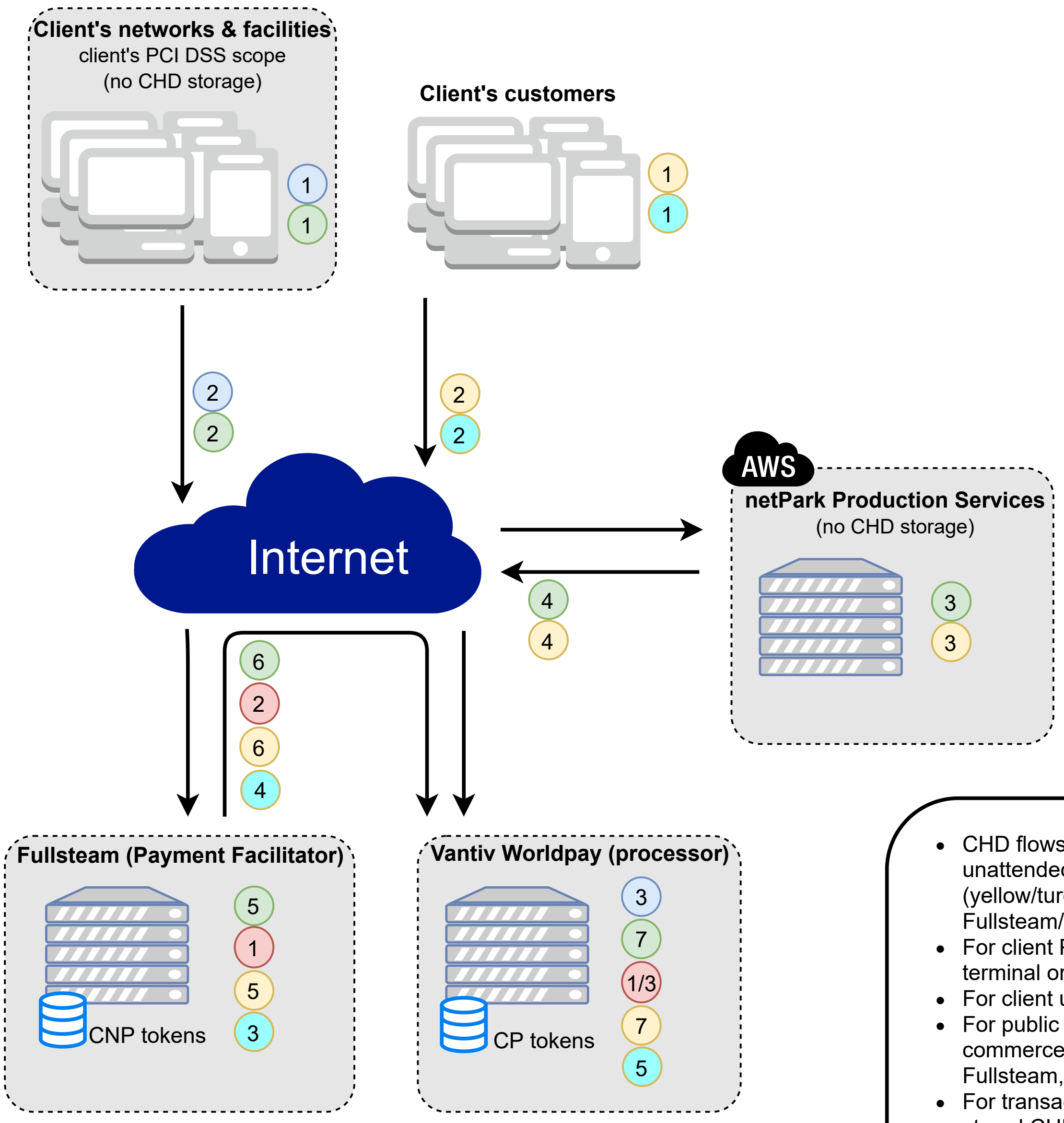
Generalized Cardholder Data (CHD) flow via netPark Pay

rev 2/16/2021

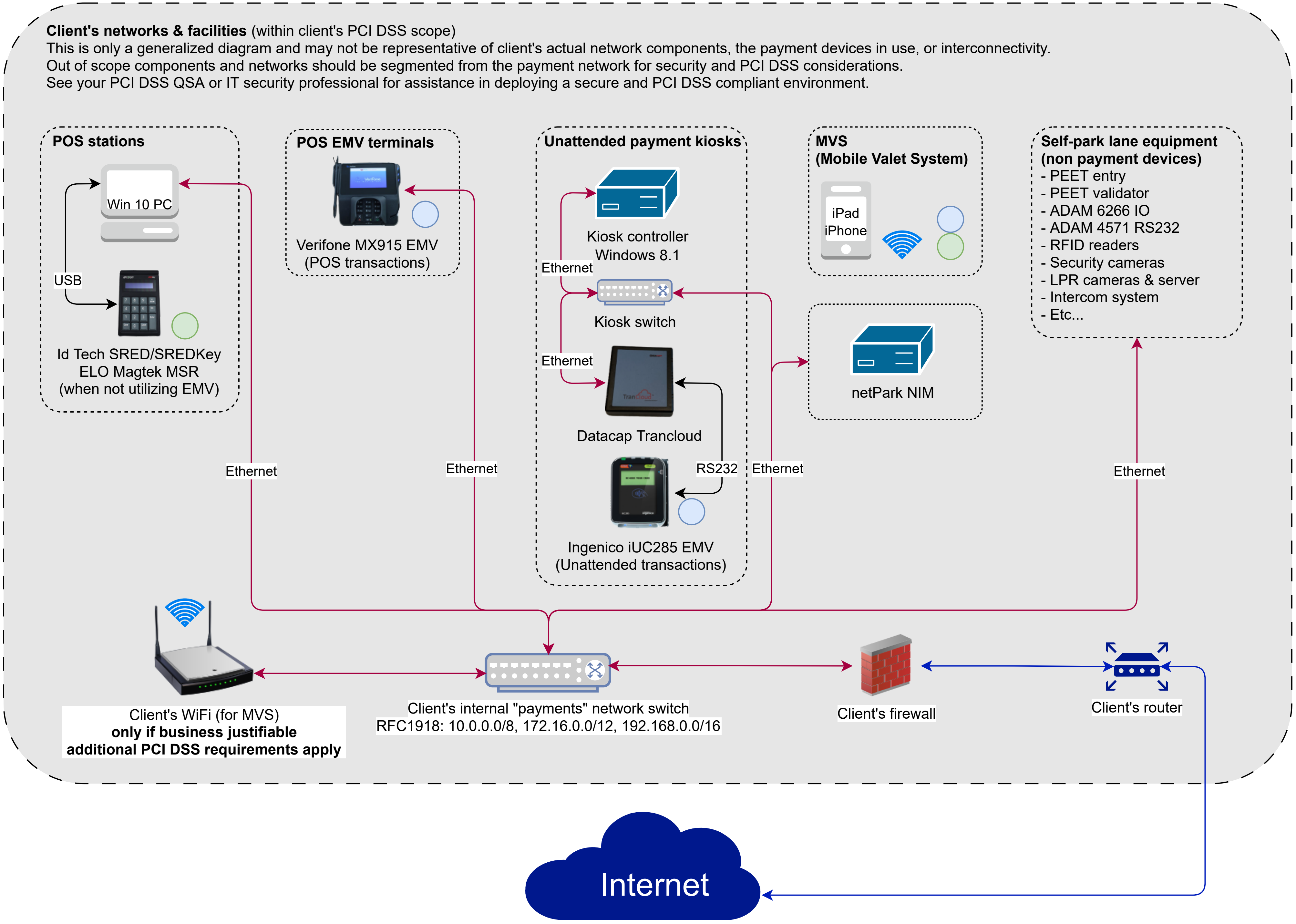


CHD transaction types

- 🔵 **Clients: EMV E2EE (POS/MVS/kiosk)**
- 🟢 **Clients: MSR E2EE (POS/MVS)**
- 🔴 **Tokenized COF: (Fullsteam/Worldpay)**
- 🟡 **Customers: keyed (websites & mobile apps)**
- ○ **Customers: keyed hosted-form (websites)**

- CHD flows originate from either a client's POS/MVS device (blue/green), a client's unattended kiosk (blue), a public client website or client mobile application (yellow/turquoise), or from previously tokenized credit cards (COF) which are stored at Fullsteam/Worldpay (red).
- For client POS/MVS devices, CHD is captured via either a Verifone MX915 EMV E2EE terminal or a MagTek/Id Tech MSR E2EE device.
- For client unattended kiosks, CHD is captured via an Ingenico iUC285 EMV E2EE terminal.
- For public client websites and mobile applications, CHD is captured through an e-commerce web/application payment form which can be hosted by either netPark or Fullsteam, depending on the application.
- For transactions based on a tokenized COF, either Fullsteam or Worldpay retains the stored CHD and it is never passed back to netPark.
- All CHD is transmitted via TLSv1.2 or later, on top of any applicable 3DES DUKPT E2EE.
- No PA DSS payment applications exist on the client's networks or facilities.
- Tokenization, authorization, and settlement occurs via the Fullsteam API and Worldpay.
- See the following pages for additional client network details.

Generalized "typical" client network via netPark Pay - not recommended due to lower security and higher PCI DSS scope



Client's networks & facilities (within client's PCI DSS scope)
This is only a generalized diagram and may not be representative of client's actual network components, the payment devices in use, or interconnectivity.
Out of scope components and networks should be segmented from the payment network for security and PCI DSS considerations.
See your PCI DSS QSA or IT security professional for assistance in deploying a secure and PCI DSS compliant environment.

POS stations

Win 10 PC

USB

Id Tech SRED/SREDKey
ELO Magtek MSR
(when not utilizing EMV)

POS EMV terminals

Verifone MX915 EMV
(POS transactions)

Unattended payment kiosks

Kiosk controller
Windows 8.1

Ethernet

Kiosk switch

Ethernet

Datacap Trancloud

RS232

Ingenico iUC285 EMV
(Unattended transactions)

MVS
(Mobile Valet System)

iPad
iPhone

netPark NIM

Self-park lane equipment
(non payment devices)
- PEET entry
- PEET validator
- ADAM 6266 IO
- ADAM 4571 RS232
- RFID readers
- Security cameras
- LPR cameras & server
- Intercom system
- Etc...

Ethernet

Ethernet

Ethernet

Ethernet

Client's WiFi (for MVS)
only if business justifiable
additional PCI DSS requirements apply

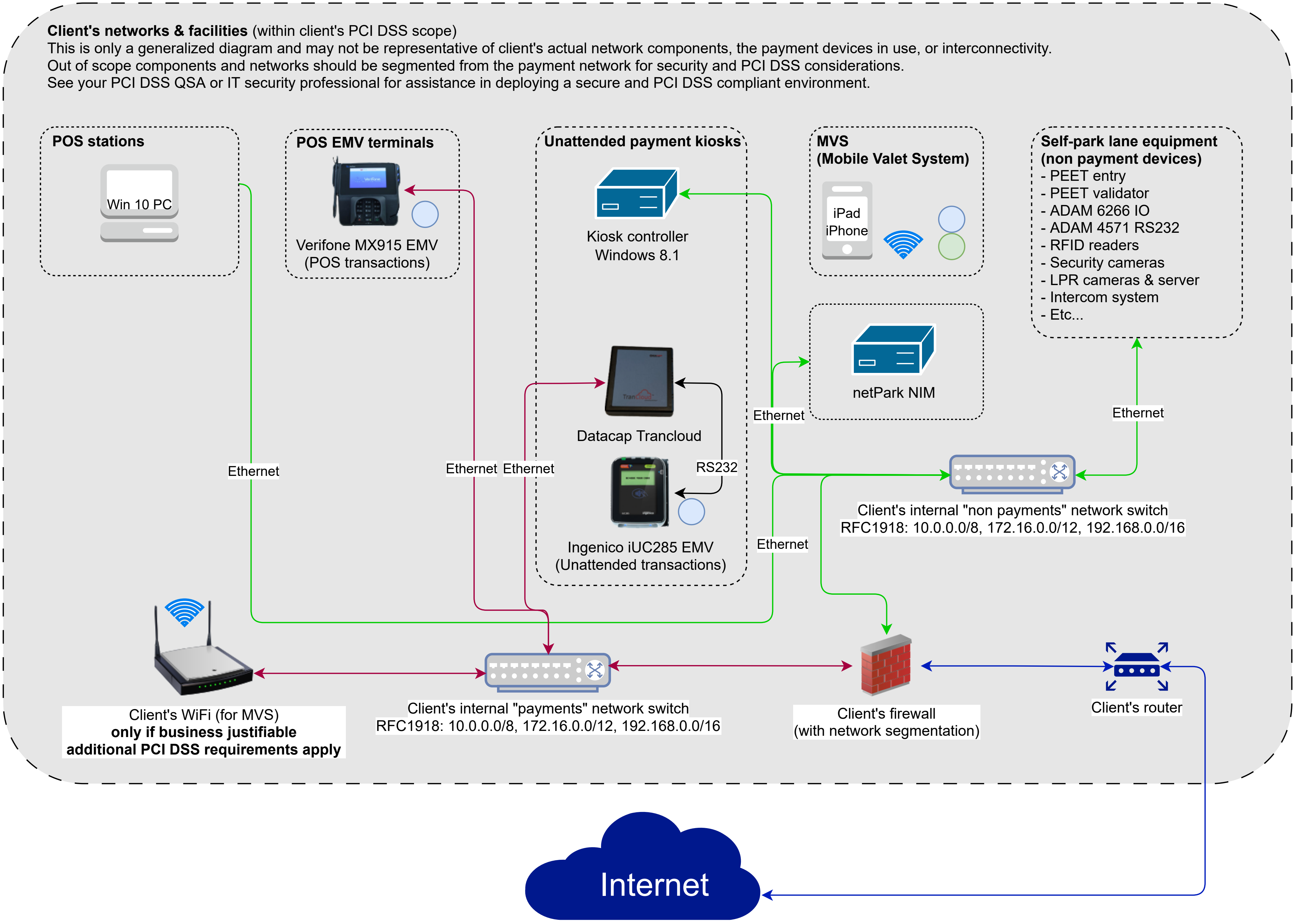
Client's internal "payments" network switch
RFC1918: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

Client's firewall

Client's router

Internet

Generalized "improved" client network via netPark Pay - recommended due to enhanced security and reduced PCI DSS scope



Client's networks & facilities (within client's PCI DSS scope)
This is only a generalized diagram and may not be representative of client's actual network components, the payment devices in use, or interconnectivity.
Out of scope components and networks should be segmented from the payment network for security and PCI DSS considerations.
See your PCI DSS QSA or IT security professional for assistance in deploying a secure and PCI DSS compliant environment.

Self-park lane equipment (non payment devices)
- PEET entry
- PEET validator
- ADAM 6266 IO
- ADAM 4571 RS232
- RFID readers
- Security cameras
- LPR cameras & server
- Intercom system
- Etc...

POS stations
Win 10 PC
POS EMV terminals
Verifone MX915 EMV
(POS transactions)
Unattended payment kiosks
Kiosk controller
Windows 8.1
Datacap Trancloud
RS232
Ingenico iUC285 EMV
(Unattended transactions)
MVS
(Mobile Valet System)
iPad
iPhone
netPark NIM
Ethernet
Ethernet
Ethernet
Ethernet
Ethernet
Ethernet
Ethernet
Client's internal "non payments" network switch
RFC1918: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
Client's WiFi (for MVS)
only if business justifiable
additional PCI DSS requirements apply
Client's internal "payments" network switch
RFC1918: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
Client's firewall
(with network segmentation)
Client's router
Internet