clover
A First Data Company

Enterprise Security Architecture - EU

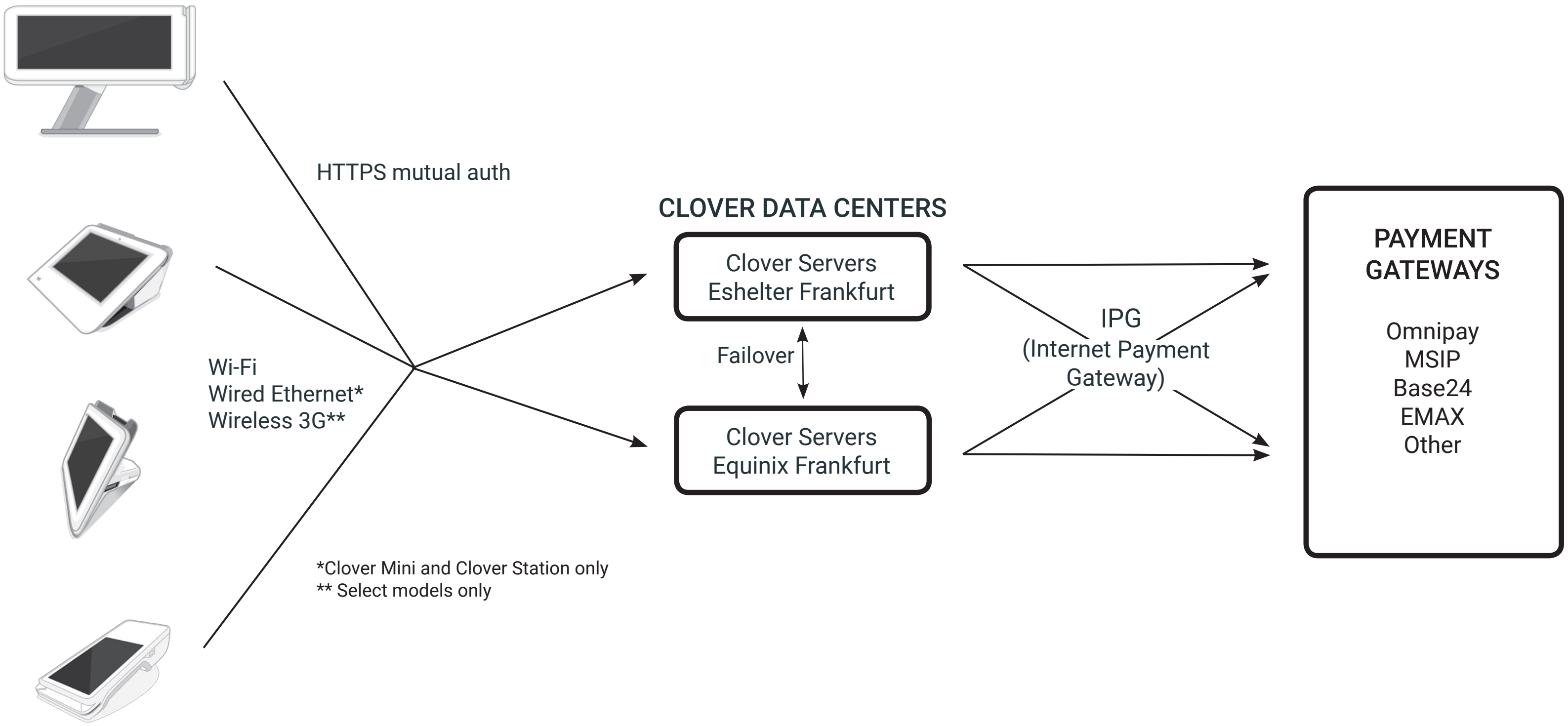
Overview

This page describes the network security architecture for Clover devices in the EU.

Clover Network Security Architecture

Clover devices can connect to Clover's servers via Wi-Fi, wired Ethernet, or 3G. Clover has two sets of redundant servers located at two separate data centers in Frankfurt, Germany. Both sets of servers have private direct connections to the different payment gateways.

Network Layout



HTTPS mutual auth

Wi-Fi
Wired Ethernet*
Wireless 3G**

CLOVER DATA CENTERS

Clover Servers
Eshelter Frankfurt

Failover

Clover Servers
Equinix Frankfurt

IPG
(Internet Payment
Gateway)

PAYMENT
GATEWAYS

Omnipay
MSIP
Base24
EMAX
Other

*Clover Mini and Clover Station only
** Select models only

ENCRYPTION

- Clover devices are SRED (Secure Read and Exchange of Data)
- All cardholder data encrypted at swipe, dip, or tap
- Cardholder data encrypted by the Secure Processor
- Data encrypted then tokenized before transmission
- 3 DES, DKUPT Public Key Infrastructure (PKI) encryption
- Tokenized data sent over TLS version 1.2

(see page 3 for details of network-supported certifications and protocols used)

HARDWARE / SOFTWARE ARCHITECTURE

- Does not use commercial off-the-shelf products
- Uses open source software products for databases applications
- Operating systems use industry-hardened Scientific Linux and Cent O/S
- Applications use Java version 8, Python scripting, and tools such as Puppet, OSSEC, and Postfix
- Network-based IDS or IPS
- Databases in a separate DMZ, protected by a Layer 4 firewall or above
- Network segmentation (e.g. VLAN, zones) used to protect network traffic, server, and data

	Clover Station	Clover Mobile/Clover Mini/ Clover Flex
Wi-Fi/BT chipsets	BCM4334-based module 802.11 a/b/g/n 2x2 MIMO, HT20/40	BCM43241-based module 802.11 a/b/g/n 2x2 MIMO, HT20/40
Supports 5GHz	Yes	Yes
Supports DFS channels (UNII-2)	Yes (Client without radar detection capability in passive scanning mode)	Yes (Client without radar detection capability in passive scanning mode)

RELIABILITY AND PERFORMANCE

- The Clover Payments processing platform operates in a hot/hot automatic failover environment with replicated Client Servers in a Primary and Secondary Data Center
- Performance managed by custom-built tools and scripts for capacity and performance management (includes caching and load balancing)
- The platform uses a type of virtualization called containerization for maximum throughput for transaction processing, data output, security, and confidentiality
- Distributed denial of service (DDoS) attack prevention and safeguards at the Data Centers with anti-DDoS mitigation or the necessary agreements to perform carrier-based or third party-based scrubbing/cleansing

TAMPER PROTECTION

- Protection mechanisms in place to prevent skimmers or fraudsters from stealing payment card data
- When tampered, the payment device enters "limited functionality mode"
- Protection mechanisms cannot be removed to fully protect merchants and cardholders

OPERATIONAL ENVIRONMENTAL REQUIREMENTS

Clover devices operate under the following environmental parameters:

- Maximum temp: 135C
- Minimum temp: -70C
- Voltage (VDD) high: 3.8V
- Voltage (VBAT) high: 3.8V
- Voltage (VBAT) low: 2.1V

Crossing these thresholds will trigger the tamper mechanisms and will require the device to be sent back to Clover.

OPERATIONS AND MAINTENANCE

- The Android kernel cannot be modified and signed by a secure key and verified by the bootloader; if modified, the device cannot boot
- Log detail: Details are logged at the user ID, event type, date/time stamp, success/ failure indication, event origin, id/name of affected data, system component or resource
- Log reports**:** Detailed audit trails for all system component activity, individual access, root/admin, access to audit trail, invalid access attempts, use of ID/authentication mechanisms, initialization of audit trails, create/delete of system level objects/ executables
- Backup/recovery data: Backups are encrypted, done online, monitored and logged. Access to backup/recovery data is monitored and logged. Clover clients update themselves automatically during their business' closed hours. This includes app updates and firmware updates

clover
A First Data Company

© 2017 First Data Corporation. All Rights Reserved.
Confidential

## Encryption and Certificates	 Clover Go	 Clover Station	 Clover Mini Clover Mobile Clover Flex
Transmission Encryption	TransArmor	TransArmor	TransArmor
Secure Read and Exchange of Data (SRED)	Yes, SRED	Yes, when paired with Clover Mini or FD40	Yes, SRED
Encrypting Key Type and Strength	3DES DKUPT	3DES DKUPT	3DES DKUPT
TLS Version and Cipher Suite	TLS version 1.2 with 3DES DUKPT	TLS version 1.2 with TLS_ECDHE_RSA_WITH_AES_25 6_CBC_SHA cipher	TLS version 1.2 with TLS_ECDHE_RSA_WITH_AES_25 6_GCM_SHA384 cipher
WI-Fi Support and Protocols	Yes, support for cellular and wireless networks	• Open Wi-Fi • WEP • WPA/WPA2 Personal • WPA/WPA2 802.1x Enterprise • PEAP, TLS, TTLS, PWD • Phase 2 authentication: None, PAP, MSCHAP,MSCHAPV2, GTC • User provided Certificates / Certificate Authorities are not supported	• WPA/WPA2 Personal • WPA/WPA2 802.1x Enterprise • PEAP, TLS, TTLS, PWD • Phase 2 authentication: None, PAP, MSCHAP, MSCHAPV2, GTC. • User provided Certificates / Certificate Authorities are not supported.
Security Certification Documents	PCI PTS Approval	Security Architecture and Specs	Clover MIni: PCI PTS Certification Clover Mobile: PCI PTS Certification Clover Flex: PCI PTS Certification

clover
A First Data Company

© 2017 First Data Corporation. All Rights Reserved.
Confidential