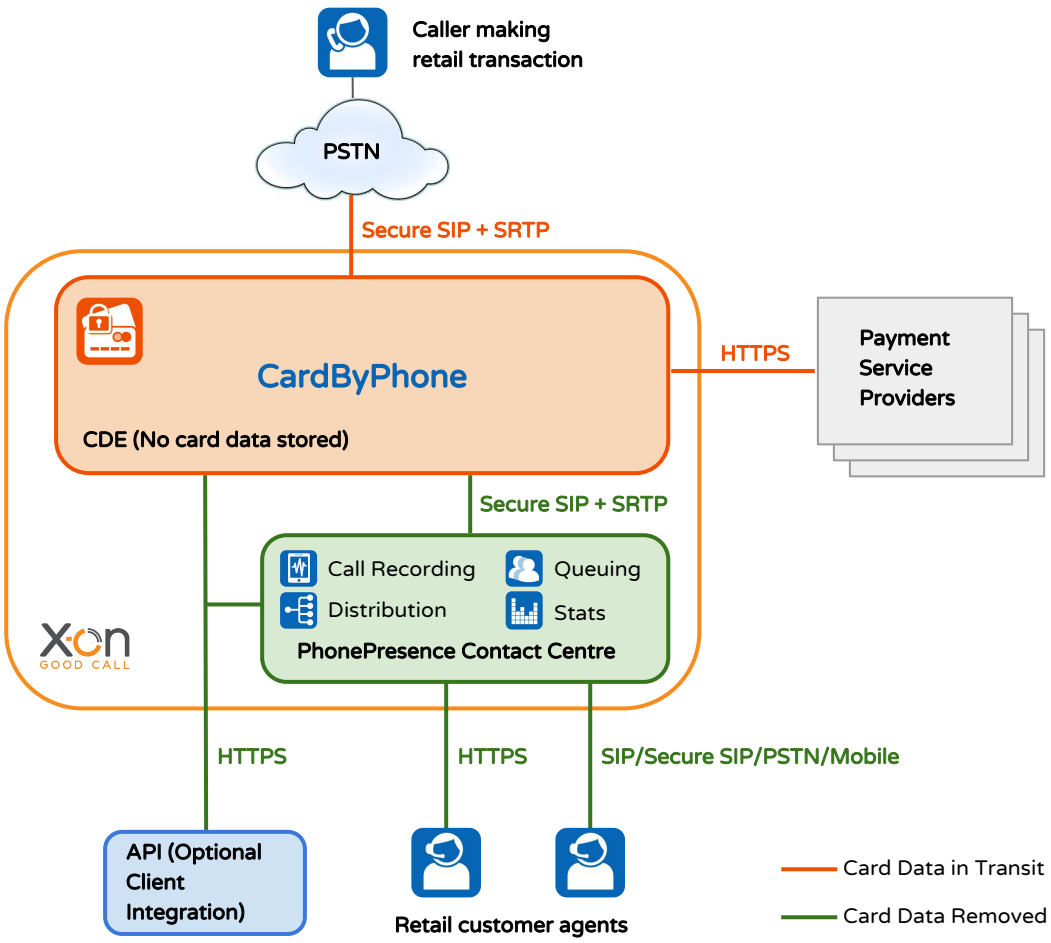
CardByPhone PCI Compliance

The following information is to assist security managers in understanding how card data security is maintained in the CardByPhone module.

The document is written with reference to PCI Data Security Standard v3.2 (PCI DSS) which underpins the design of the service and policies under which it is operated. This is a summary of certain information contained within these maintained policies and associated documentation but is not fully comprehensive.

System Architecture

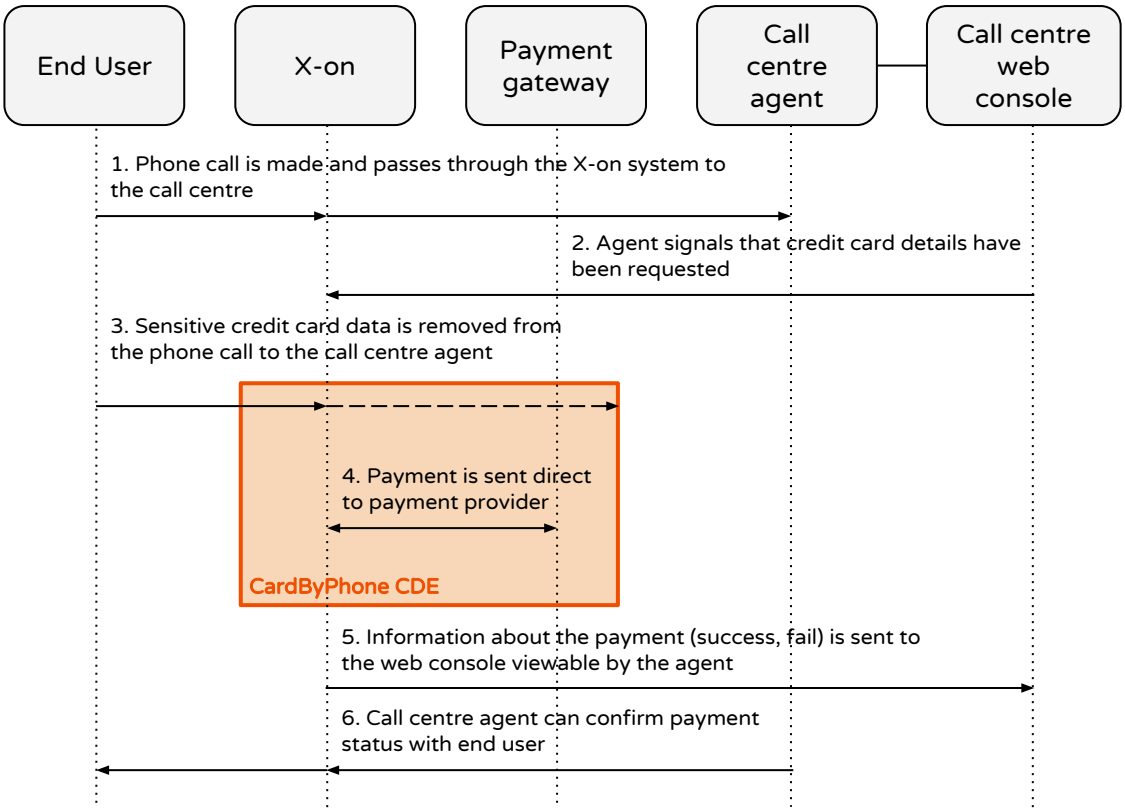
The CardByPhone service is built in a secure Card Data Environment (CDE) which is physically and logically isolated from other parts of X-on's data centres. The following data flow overview shows how cardholder data is constrained.



x-on.co.uk
0333 332 0000

Data Flow

This diagram describes the data flow during a typical card transaction:



Information Security Policy

This is some key points extracted from X-on's policy in relation to Section 12 of the PCI DSS requirements v3.2. A full version of the current policy is published to be available customers contracting to the CardByPhone service.

General

- X-on maintains a security policy which is reviewed annually and when changes are made to the service (12.1)
- X-on maintains a formal risk assessment process which is reviewed quarterly. This is combined with X-on's compliance to ISO27001. (12.2)
- Usage policies for critical technologies are maintained together with acceptable use (12.3).
- Security policies define responsibilities for all personnel responsible for maintenance of the CardByPhone environment (12.4). Executive Management take overall responsibility for protection of cardholder data (12.4.1).
- Security policies define roles for managing and disseminating policies and procedure, including training, review and new starter processes. (12.5, 12.6, 12.7).

x-on.co.uk
0333 332 0000

Policy Regarding Third Party Service Providers (12.8)

X-on maintains a list of third party service providers involved in the transmission of cardholder data. All current service providers are payment gateways (payment service providers) who are audited against PCI DSS Level 1. X-on will check their status annually. Customers wishing to deploy CardByPhone with payment providers who are not Level 1 compliant will need to discuss commercial terms relating to X-on's due diligence in engaging with the provider.

Acknowledgment of Responsibility (12.9)

X-on's contract with customers will state that we take responsibility for cardholder data while it is being transmitted via the X-on network. X-on will never store cardholder data.

Phone calls from network operators which may contain cardholder data must be transmitted to the Card Protected Environment withing X-on's data centres to a Network Termination Point via PSTN or encrypted SIP (specifically SIPS using TLS 1.2 and SRTP).

More Information

X-on's Qualified Security Assessor (QSA) organisation is IT Governance.

All enquiries regarding PCI DSS compliance should be made in the first instance to X-on's Head of Information Security, Callum Guy (callum.guy@x-on.co.uk).

Enquiries regarding features and functionality of the CardByPhone and PhonePresence hosted contact centre service should be made to your nominated Account Manager.