How cryptographic key management is handled in NCR Secure Pay

Article Number: 457 | Rating: Unrated | Last Updated: Thu, Aug 28, 2014 at 11:43 AM

Summary: How is cryptographic key management handled in NCR Counterpoint with Secure Pay and who has access to the encryption keys?

Solution: Previously NCR Counterpoint used Blowfish encryption keys to encrypt credit card information when using CPGateway.Â This is no longer used with NCR Secure Pay since credit card information is tokenized and only the token is stored in the database. NCR Secure Pay uses a private key encryption system. Only the private keys can decrypt credit card information and they only exist on the P2PE device and a Hardware Security Module (HSM) at the NCR Secure Pay host. Â Â This is fundamentally more secure than CP Gateway encryption since the information needed to decrypt data does not exist in the NCR Counterpoint application or database.P2PE keys are unique per device. This means that, in the extremely unlikely event that a private key was compromised, it would only impact a single device. Only Monetra and our key administrator can access these keys.Â No reseller, merchant, or other personnel at NCR has access to this information. At the transaction level, DUKPT key management is in use, which generates a unique key for each transaction; it is the same key management that is used to manage PIN debit keys. Â Â

Posted - Thu, Aug 21, 2014 at 5:21 PM. This article has been viewed 1653 times.
Online URL: https://counterpoint.knowledgebase.co/article-457.html