August 7, 2016

FAQs

1. **How does Samsung Pay work?**
   Each time Samsung Pay is used for a transaction, the Samsung Pay handset sends at least three pieces of information.

   The first is a digital token that represents the credit or debit card information. The digital token is a surrogate credit or debit card number. The digital token's primary purpose is to route transactions to the correct payment network and to the correct issuer.

   The second piece of information is the application transaction counter (ATC). The ATC is a counter that is updated for every transaction. Its purpose is to help ensure that the same transaction information cannot be replayed to make multiple purchases. Payment networks use this number to track the sequence of transactions and determine whether an attempted transaction is older than the last one approved or is otherwise out of sequence. If so, it is an indication that something is amiss, and appropriate action can be taken.

   The third piece of information is the cryptogram. The cryptogram is an authentication code generated using, at a minimum, a secret key, the digital token and the ATC. Cryptograms serve to validate that the transaction information has not been modified and that it was generated by the expected user's handset.

2. **What is a token and how is it generated?**
   A digital token is created to represent consumers' payment credentials. By substituting the real card number with a token, Samsung Pay avoids putting the real card numbers at risk of theft and misuse. Like credit and debit card numbers, the purpose of the digital token is to route transactions to the correct payment network and issuer. Samsung Pay does not store credit or debit card numbers. Instead, Samsung Pay uses tokens for transactions. Tokens are generated by the payment network, and not by the Samsung Pay handset. The card issuers and payment networks set the rules and parameters of the tokenization service, conduct account verification and cardholder authorization during the token request stage (when the token is provisioned), and authorize transactions.

3. **How is a cryptogram generated?**
   A cryptogram is generated using at least three pieces of information: the digital token, the application transaction counter (ATC), and a secret key. The cryptogram is designed to appear fully random to anyone that does not have the secret key. This works to prevent a cryptogram from being guessed. The secret key is generated by the payment networks and is protected, end to end, between the payment networks and TrustZone on the device. Only one cryptogram can be generated per explicit user authorization. The cryptograms are used to tie an ATC to a digital token and help to prevent modification of the ATC. This in turn helps to prevent transaction information used for one purchase from being reused for multiple purchases.

4. **Is it possible for a hacker to steal a token and make a payment?**
   Samsung Pay uses tokenization to substitute card numbers with tokens provided by payment networks. These tokens cannot be converted back to the original card numbers except by the payment networks, and so stolen tokens have no impact on the underlying cards. The tokens that Samsung Pay receives can also be distinguished from regular credit and debit card numbers by the payment networks. Use of a Samsung Pay token indicates to the payment network that a valid cryptogram is required before the transaction can be processed. Since cryptograms can only be generated using a secret key, and since the secret key is known only to TrustZone and

the payment networks, stolen tokens alone cannot be used to make payments.

5. **How does Samsung Pay handle tokens to ensure user information is safe and secure?**
Two factors differentiate Samsung Pay from other mobile wallets: leverage of TrustZone, and deep integration with the Samsung Knox platform.

TrustZone is hardware-based security built right into the chip. The keys used to generate cryptograms, and the keys used to securely communicate with payment networks, are designed to be accessible only in TrustZone. In addition, Samsung Pay-capable devices come with a hardware-backed key that is unique to that device. It is this device-unique hardware key that distinguishes TrustZone's secure-use area from the device's normal-use area. In other words, this hardware-backed key is the sole gateway to Samsung Pay keys on the device, and only TrustZone may access the hardware-backed key.

Samsung Knox is a platform for security enhancements that span from the Android app level all the way to TrustZone. In part, Samsung Knox provides firmware information to TrustZone components during a process called Trusted Boot. TrustZone leverages this information to try to determine whether it is safe to make Samsung Pay keys available for use. Samsung Pay is designed to render user data and payment card data protected by these keys inaccessible when TrustZone determines that the device is in an unsafe state.

6. **Do tokens share similarities in the generation process, making it possible for hackers to guess the next tokenized number knowing the previous one?**
The digital token itself cannot make payments through transactions and each payment needs at least three pieces of information including a digital token, an application transaction counter (ATC) and a cryptogram. Tokens are not intended to be random or difficult to guess. Proof of authorization lies instead with the cryptogram. Cryptograms are intended to be difficult for hackers to guess.

7. **Is it possible to make purchases with a "skimmed" token?**
The possibility of a Samsung Pay user transmitting a payment token using user authentication such as fingerprint, having a fraudster capture the data on a separate device, and the fraudster relaying the token at a credit card reader for a successful transaction is extremely unlikely. In order for this "token skimming" to work, multiple difficult conditions must be met. First the user must permit the token and cryptogram generation with his or her own authentication method. This pair of token and cryptogram (also known as a "payment signal") must be transmitted to the POS for each transaction and cannot be used for multiple transactions.

Then the fraudster needs to capture the signal on a device that is within very close proximity to the Samsung phone. Due to the short-range nature of MST, it is difficult to capture the payment signal. Even if the fraudster was able to capture the signal, the fraudster would have to ensure that the original payment signal of the legitimate user does not get to the issuer for approval. Otherwise the captured signal would be useless. Ensuring this may require the fraudster to jam the connection between the phone and POS terminal or to quickly complete the transaction before the legitimate user's signal reaches the payment terminal and the card issuer. Because users typically permit the cryptogram generation just before their payment at the POS, these conditions would be very difficult to meet in practice. When any transaction happens, the legitimate Samsung Pay user would get immediately a Samsung Pay transaction notification on the smartphone screen. The users would take any necessary action with his or her issuer with payment transaction including un-familiar one.

In summary, Samsung Pay's multiple layers of security make it extremely difficult to make a purchase by skimming a token.

Note: This skimming attack model has been a known issue reviewed by the card networks and Samsung pay and our partners deemed this potential risk acceptable given the extremely low likelihood of a successful token relay attack. The card networks and issuers also run their fraud prevention algorithms on all payment attempts, including Samsung Pay. This serves as another layer of protection against token relay.

##########