EMV Transaction Aspects
Card Payment Experience

Performing a transaction with both the merchant and the cardholder present

CHIP TECHNOLOGY

Today, an increasing number of payment options are based on chips embedded into the device which the consumer uses to pay a merchant. The most common of these devices is still the 'chip and PIN' plastic card which has been with us for well over a decade. Increasingly though, the same chip technology, in combination with different forms of communication, is being used to give consumers more flexible ways of paying. Examples include the same chip and PIN card being 'tapped' on a contactless interface instead of inserting in a reader. Other methods gaining in popularity include the use of the smartphones that are in many consumers' pockets, operating over Near Field Communication (NFC) to perform contactless transactions based on cards stored in a 'wallet' downloaded on to the phone or other mobile device. Another growth area is 'wearables' where again the same chip technology is embedded into a device which the consumer may carry or wear, such as a smartwatch, or a ring. This gives merchants and consumers much more flexibility in terms of speed and convenience during checkout, whilst extending the security afforded by chip based transactions into new environments such as mass-transit, parking, vending and many others.

CARD ISSUING

Many aspects of a card-based transaction 'journey' begin well before a card reaches the hand of the consumer. When a customer signs a contract with a card issuer, they will have agreed what product this is for. It could be a debit card linked to a customer's bank account, or a credit card linked to a new line of credit. It could even be a card with both credit and debit accounts embedded in the chip. It could also be a card that is known as 'co-badged'. This is where a single account can be used with two different brands, usually a local brand together with an international one.

Issuers must take into consideration other factors when programming cards. For example, recent European regulations require that when a customer is using a co-badged card, the merchant and the cardholder have more say over which scheme rules should be used in a transaction. Similarly, those regulations require in some cases that a cardholder 'proves' that

THIS DOCUMENT WAS ORIGINALLY PUBLISHED BY THE ECSG IN 2018.

it is them using their card by performing 'Strong Customer Authentication' (SCA) according to criteria set out in the regulation. Presenting their card and entering their PIN is an example of a consumer performing SCA. Support for both of these regulatory requirements can be met, at least partially, through settings programmed into the chip.

On top of these regulatory requirements, issuers also programme into the chip rules to help manage risk, based on their own risk appetite. Risk criteria can vary dependant on the type of product they have issued, where the card can be used or even whether the card can be used to withdraw cash from an ATM.

This flexibility means that the rules contained within the chips can be quite complex. However, most of this complexity is transparent to both the consumer and the merchant, the impact to the consumer will usually be to select which product they want to use, and to enter their PIN if required.

Whilst the issuer programs rules into the chip before it is issued to the consumer, it is not until a transaction is performed that the chip knows which of the rules should be implemented, and how. This, in conjunction with other rules programmed into the point of sale by the merchant's acquirer, will determine what the consumer actually sees, and must do, when the transaction is performed.

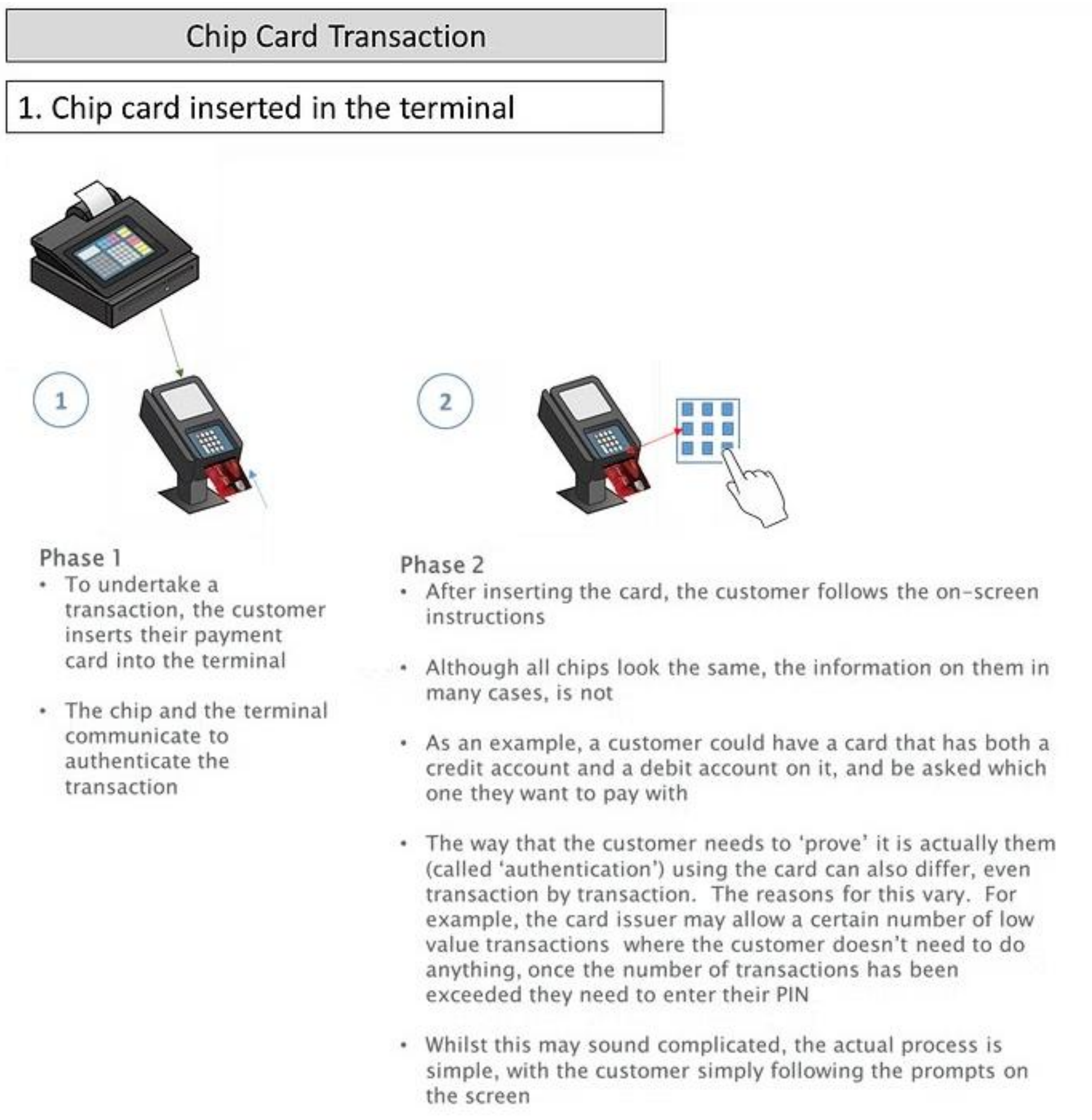
PERFORMING A TRANSACTION

In most environments a transaction will follow a standard process. The transaction amount for the goods or services the consumer is buying will be totalled up on the point of sale and the consumer will be asked to present their card. Remember the 'card' could be a plastic card, a mobile phone or a wearable. Depending on the transaction amount, or how the customer wants to pay, they will either physically insert or tap their card. Usually, the terminal will display the transaction amount prior to the customer presenting their card. This is to allow the customer to confirm that they agree with the transaction amount before continuing with the transaction. There are some circumstances where it is not possible to display the transaction amount, such as in a mass transit environment, but there are specific rules governing these types of situations.

When the card is presented, in addition to the customer and merchant providing their inputs (e.g. transaction amount and PIN), the chip and the terminal perform a number of security checks. Using cryptography, the card and the terminal can check that each device is genuine. At the same time, the card and the terminal will be examining the issuer's rules contained within the chip on the card and the rules the acquirer has set in the terminal. These rules can determine, based on several factors, how the rest of the transaction should be performed. Factors include the transaction amount or the number of transactions since the customer last entered their PIN, and many others. However, complex these checks may seem, they are actually transparent to the consumer, who may simply be asked to enter their PIN or to physically enter the chip card into the terminal.

The following diagrams illustrate the three main ways a payment may occur.

1) **When using a plastic card, the customer can simply insert it in the terminal.**



Chip Card Transaction

1. Chip card inserted in the terminal

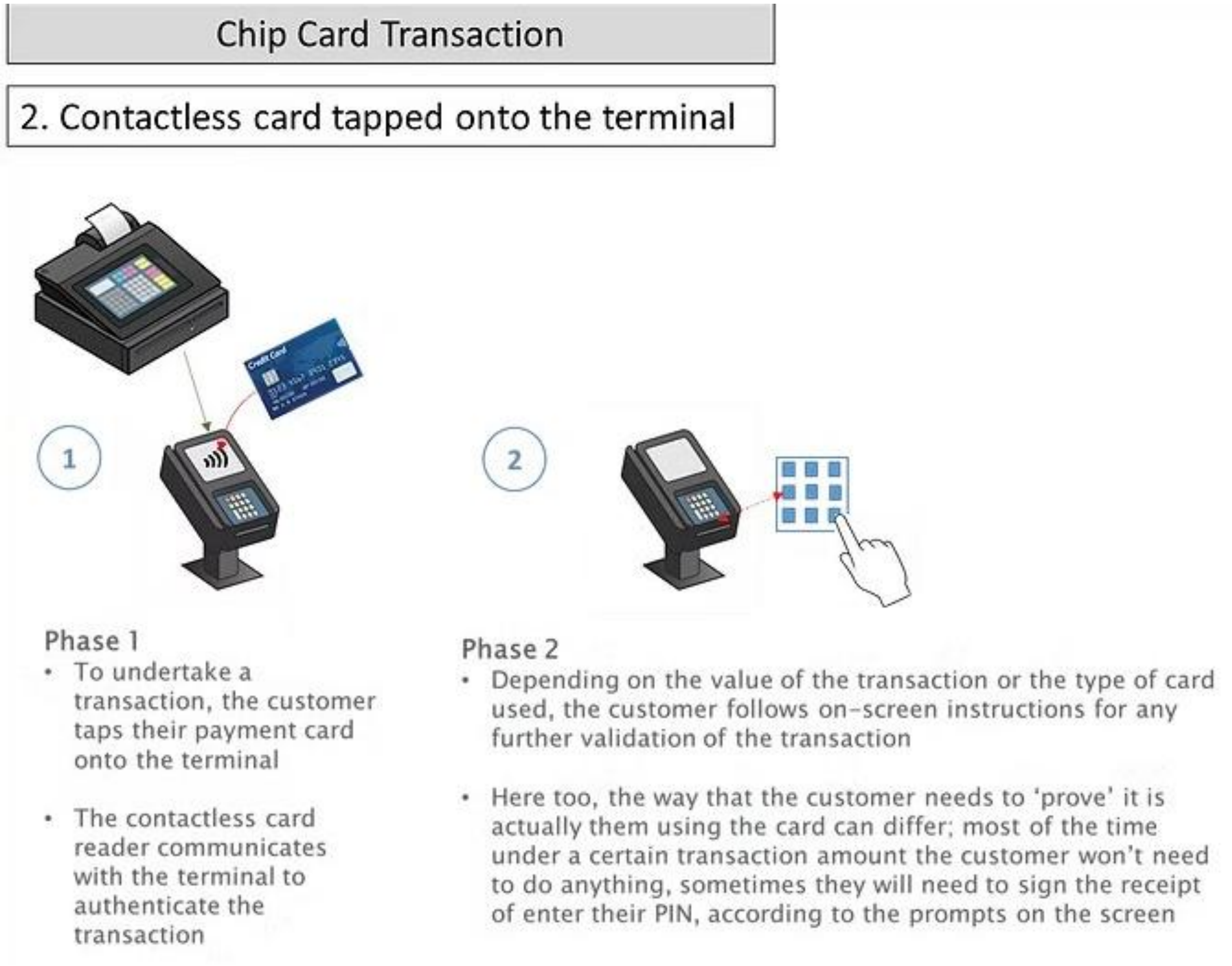
Phase 1

- To undertake a transaction, the customer inserts their payment card into the terminal
- The chip and the terminal communicate to authenticate the transaction

Phase 2

- After inserting the card, the customer follows the on-screen instructions
- Although all chips look the same, the information on them in many cases, is not
- As an example, a customer could have a card that has both a credit account and a debit account on it, and be asked which one they want to pay with
- The way that the customer needs to 'prove' it is actually them (called 'authentication') using the card can also differ, even transaction by transaction. The reasons for this vary. For example, the card issuer may allow a certain number of low value transactions where the customer doesn't need to do anything, once the number of transactions has been exceeded they need to enter their PIN
- Whilst this may sound complicated, the actual process is simple, with the customer simply following the prompts on the screen

2) If the card has a contactless function, they can simply tap it onto the terminal.



Chip Card Transaction

2. Contactless card tapped onto the terminal

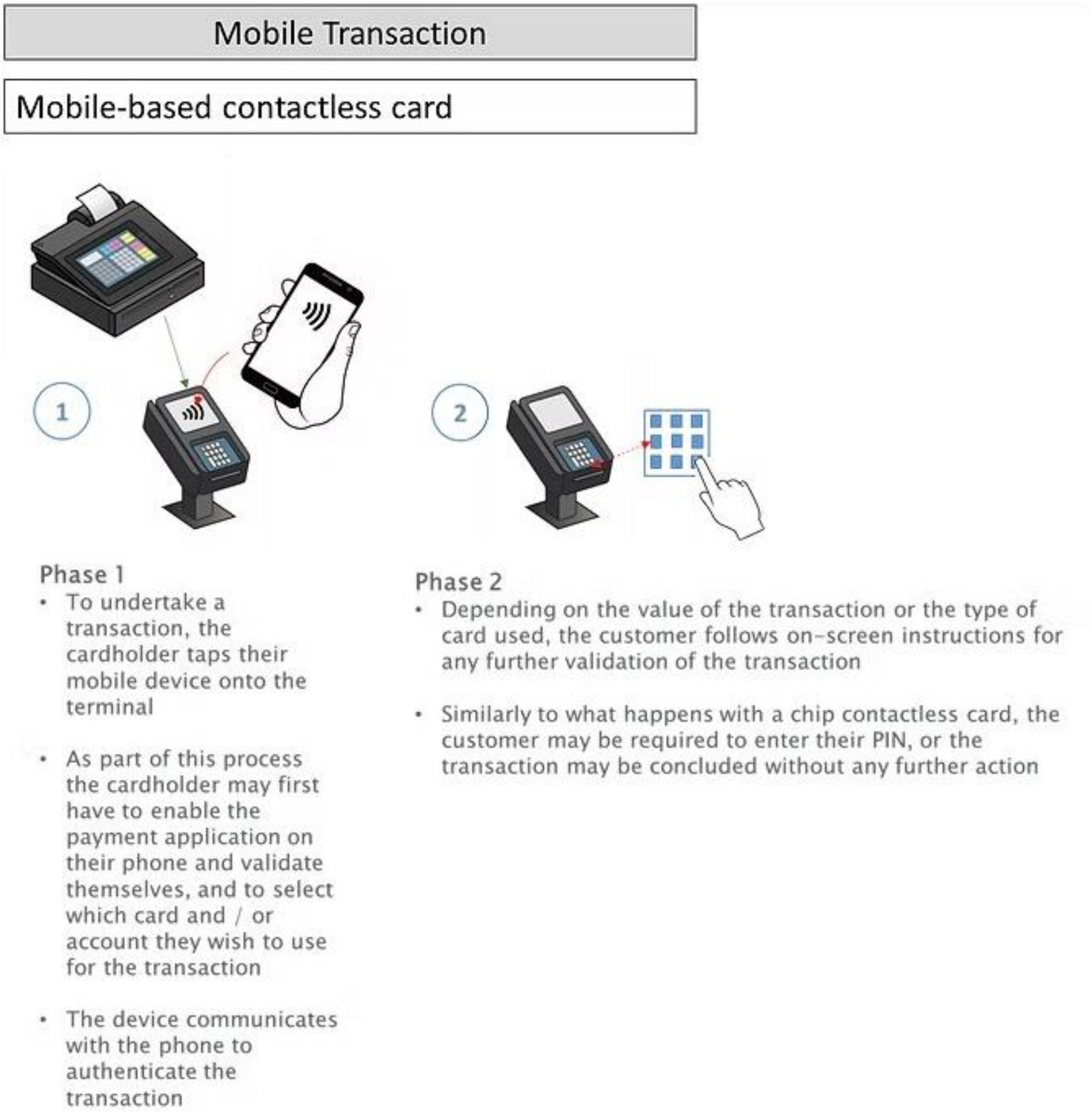
Phase 1

- To undertake a transaction, the customer taps their payment card onto the terminal
- The contactless card reader communicates with the terminal to authenticate the transaction

Phase 2

- Depending on the value of the transaction or the type of card used, the customer follows on-screen instructions for any further validation of the transaction
- Here too, the way that the customer needs to 'prove' it is actually them using the card can differ; most of the time under a certain transaction amount the customer won't need to do anything, sometimes they will need to sign the receipt of enter their PIN, according to the prompts on the screen

3) **When using a smartphone, the experience is very similar to using a contactless card.**



Mobile Transaction

Mobile-based contactless card

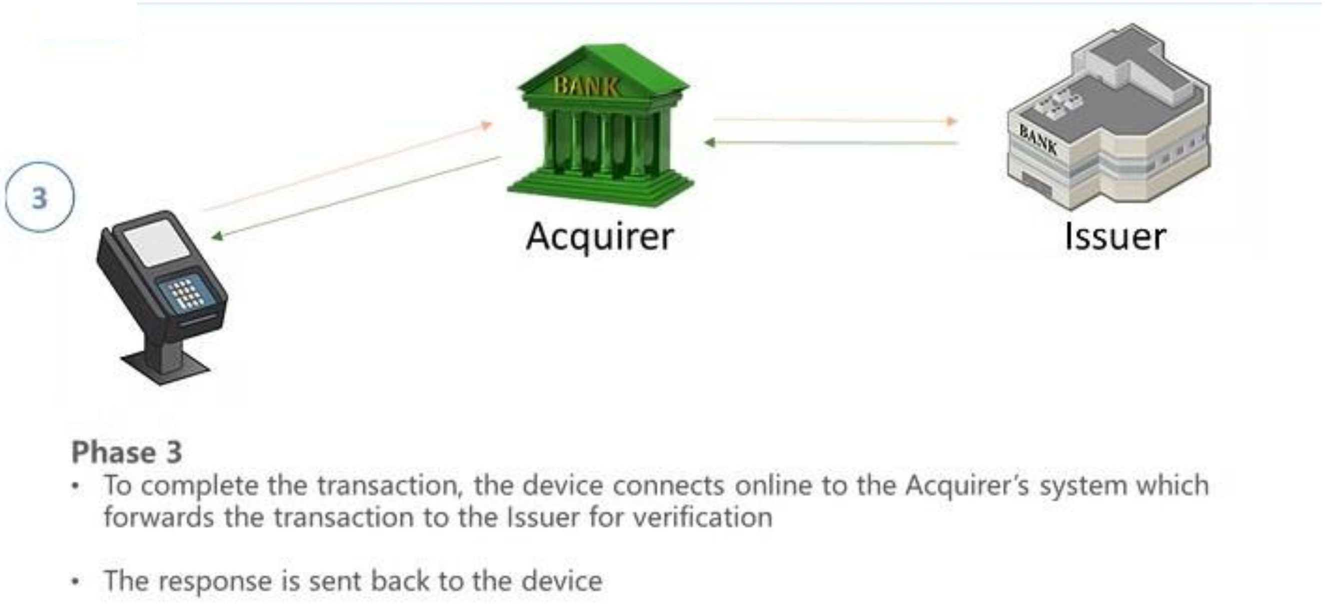
Phase 1

- To undertake a transaction, the cardholder taps their mobile device onto the terminal
- As part of this process the cardholder may first have to enable the payment application on their phone and validate themselves, and to select which card and / or account they wish to use for the transaction
- The device communicates with the phone to authenticate the transaction

Phase 2

- Depending on the value of the transaction or the type of card used, the customer follows on-screen instructions for any further validation of the transaction
- Similarly to what happens with a chip contactless card, the customer may be required to enter their PIN, or the transaction may be concluded without any further action

Whilst the transaction is being performed, and transparently to the customer, the terminal may also be communicating electronically with the issuer to perform additional (online) checks. The decision whether to communicate with the issuer will have been based on the rules mentioned earlier. Again, using cryptography, these online checks allow an issuer to check that the transaction data has not been manipulated by a bad actor and was performed using a genuine card. If the consumer has entered their PIN the issuer is able to determine whether the correct PIN has been entered. Once the checks have been successfully completed, the issuer usually sends back a message to the terminal authorising the purchase.



Phase 3

- To complete the transaction, the device connects online to the Acquirer's system which forwards the transaction to the Issuer for verification
- The response is sent back to the device