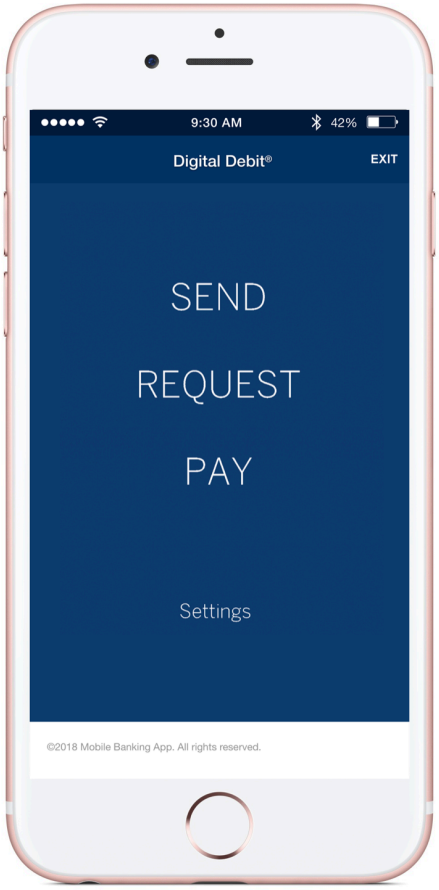
DIGITAL DEBIT®

For Real-Time Payments



Mobile App Panel Specification

Version 1.0
August 2018

Digital Debit® Version 1.0 transaction GUI - U.S. Patent D826955

Please visit our R&D website www.digitaldebit.com

Table of Contents

1 INTRODUCTION

The Digital Debit® add-on panel specification supports the Digital Debit® Group license for partners building applications meeting the ISO 20022 standard for Real-Time payments. The Digital Debit® add-on panel is cross-platform compatible with existing Apple iOS and Google Android FI mobile Apps.

.

1.1 Prerequisites

This document is a third-party addendum to The Clearing House® RTP® Credit Transfer Message Specification (Version 2.2).

The Clearing House® and RTP® are registered trademarks of The Clearing House Payments Company LLC.

Digital Debit® is a registered trademark of Qondado LLC.

All trademarks used in this specification constitute Nominative Fair Use.

2 Functionality

Digital Debit® is a mobile transaction panel for existing Financial Institution mobile applications to add a QR transactional front-end to The Clearing House® RTP® Credit Transfer Message protocol payment rail hooks.

Please Note: Digital Debit® Group does not provide programmatic access to the RTP® system. Licensed developers are required to use the Digital Debit® Panel SDK for iOS and Android as the foundation for panel installation.

Licensed developers are also required to protect their mobile app using standard banking user entry methods such as:

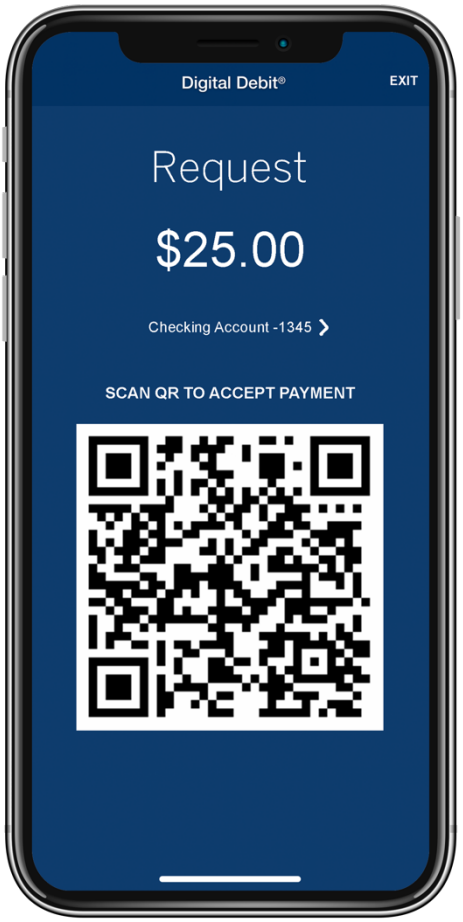
- Username and Password
- App access PIN code
- Biometric authentication

Reference Definition:

Dagnus is the Pay-to-Scan QR endpoint registration system that administer KodeKey tokens for:

- User QR – for donations, small business merchants and singular pay stations.
- Merchant QR – for point-of-sale terminals
- ATM QR – for ATM and bank teller terminals

3 P2P Request Mode



Scan the QR above to see XML format.

Exit button to the host App panel.

User entry field for amount to request from a sending user. **With device-to-device transactions, both sending and requesting users must enter the same amount to mutually agree to the transaction.**

User entry field for source account selection to send and receive funds from.

The Dynamic QR must be customized by the developer to contain an encrypted RTP® Institution ID and the user's Tokenized Account Number.

Digital Debit® QR XML Format for RTP® payload:

<RTPID>AES256 Base64 Bank ID</RTPID>
<RTPT>AES256 Base64 Account Token</RTPT>

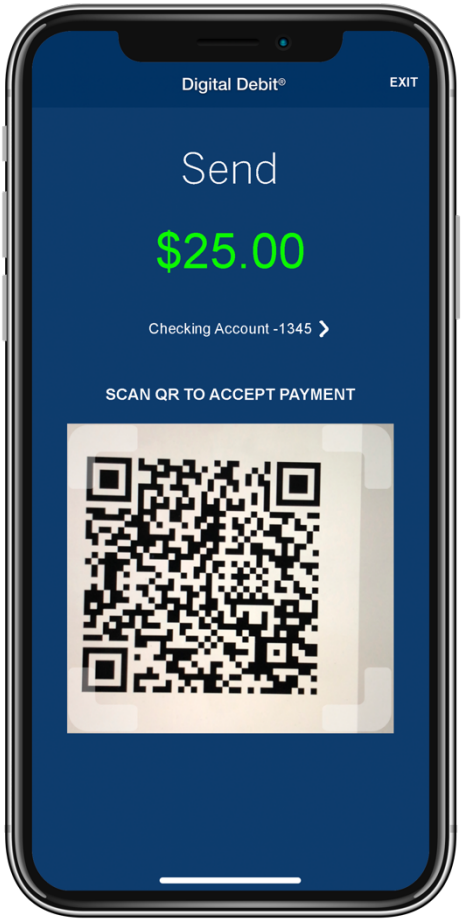
**The AES256 key should be stored on the developer application server and never in the hosting app build. The QR should be regenerated with a 1 second accurate live application server hosted AES key rotation. The application server should encrypt all payload text before the app constructs the XML formatted QR payload.*

A scan of the QR by the sending device should capture the encrypted XML payload, decrypt it on the application server (never on the user's mobile device) and process the RTP® application server transaction.

For a device-to-device QR scan, the scanned QR RTP® XML Payload is the receiver account.

Below the amount entry field, users must be able to select which RTP®-enabled banking account to use with Digital Debit®. The user selection should be saved in the app memory until the user makes another selection or reinstalls the app.

3.1 P2P Send Mode



User Entry - green color text indicates funds are available, and red color text indicates funds are not available. The QR scanner is enabled when the text is green. **With device-to-device transactions, both sending and requesting users must enter the same amount to mutually agree to the transaction.**

NOTE: Available account funds should never be visible in the Digital Debit panel.

Scanner opens when user enters an amount to send.

The sending device will collect the scanned QR XML data to deliver both the sender and receiver RTP® information to the developer's application server.

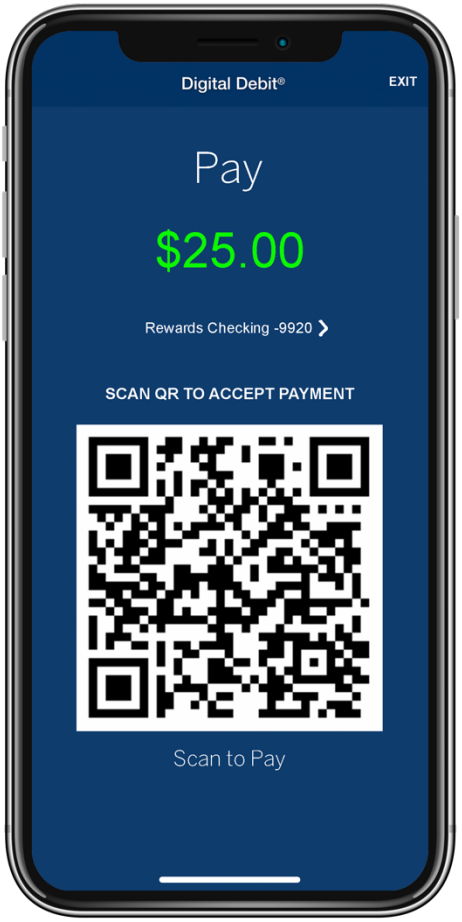
For Scan-to-Pay Registered User QR codes

The QR XML for registered User Pay-to-Scan QR code should be created with the KodeKey token issued for the verified user profile endpoint in the DAGNUS repository:

<DDU>kodekeyTOKEN</DDU>

Below the amount entry field, users must be able to select which RTP®-enabled banking account to use with Digital Debit®. The user selection should be saved in the app memory until the user makes another selection or reinstalls the app.

3.2 Merchant Pay Mode



User Entry - green color text indicates funds are available, and red color text indicates funds are not available. The QR scanner is enabled when the text is green.

NOTE: Available account funds should never be visible in the Digital Debit panel.

User's QR is the default display for Pay mode for merchant PoS scanner operation. User is required to enter the amount to pay to authorize the transaction scan.

Users can also select "Scan to Pay" button to manually open the QR scanner to scan a Digital Debit Merchant QR to complete the transaction.

A scan of the QR by the merchant Point-of-Sale (PoS) should capture the encrypted XML payload, decrypt it on the application server (never on the user's mobile device) and process the RTP® application server transaction:

For a merchant PoS scan, the scanned QR is the sending account to the merchant's RTP® account.

The merchant PoS should also be enabled to perform a QR scan to the user account to push a credit (similar to the device-to-device action) in order to issue an instant refund.

For Scan-to-Pay Registered Merchant QR codes

The QR XML for registered Merchants should be created with the KodeKey token issued for the PoS location endpoint in the DAGNUS repository:

<DDM>kodekeyTOKEN</DDM>

Note: Merchants are required to register for a KodeKey token for each Merchant terminal endpoint implementing Digital Debit®.

Below the amount entry field, users must be able to select which RTP®-enabled banking account to use with Digital Debit®. The user selection should be saved in the app memory until the user makes another selection or reinstalls the app.

4 ATM Mode

Digital Debit® ATM Mode is a device authenticator for ATM and bank customer service transactions.

Digital Debit® ATM Mode is activated when a user enters an amount to withdraw in the Digital Debit® Send panel and scans a QR on the ATM screen or at a bank teller station. Users can also scan an ATM QR with the Send Mode scanner at an amount of $0.00 to activate the device authenticator for bank teller customer service.

The Digital Debit device authenticator should also be able to operate by a bank customer service call center system using the user's registered mobile number with the host banking App.

For Registered ATM QR codes

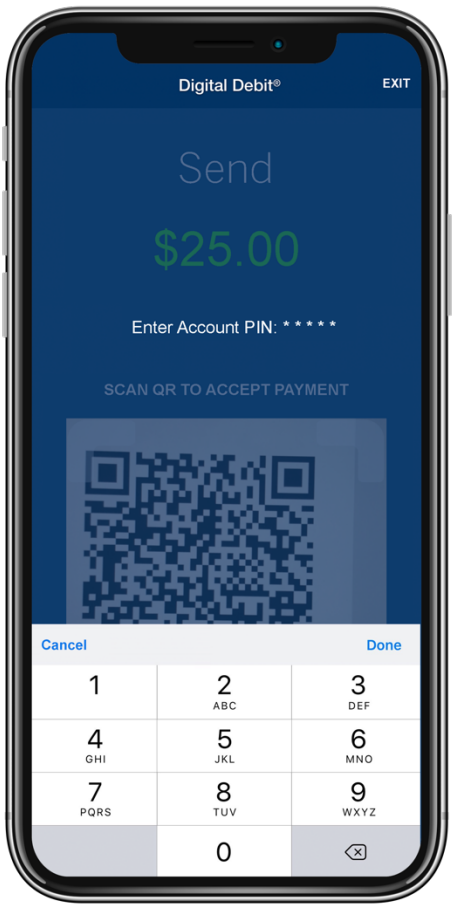
The QR XML for ATMs and bank teller stations should be created with the KodeKey token issued for the location endpoint in the DAGNUS repository:

<DDATM>kodekeyTOKEN</DDATM>

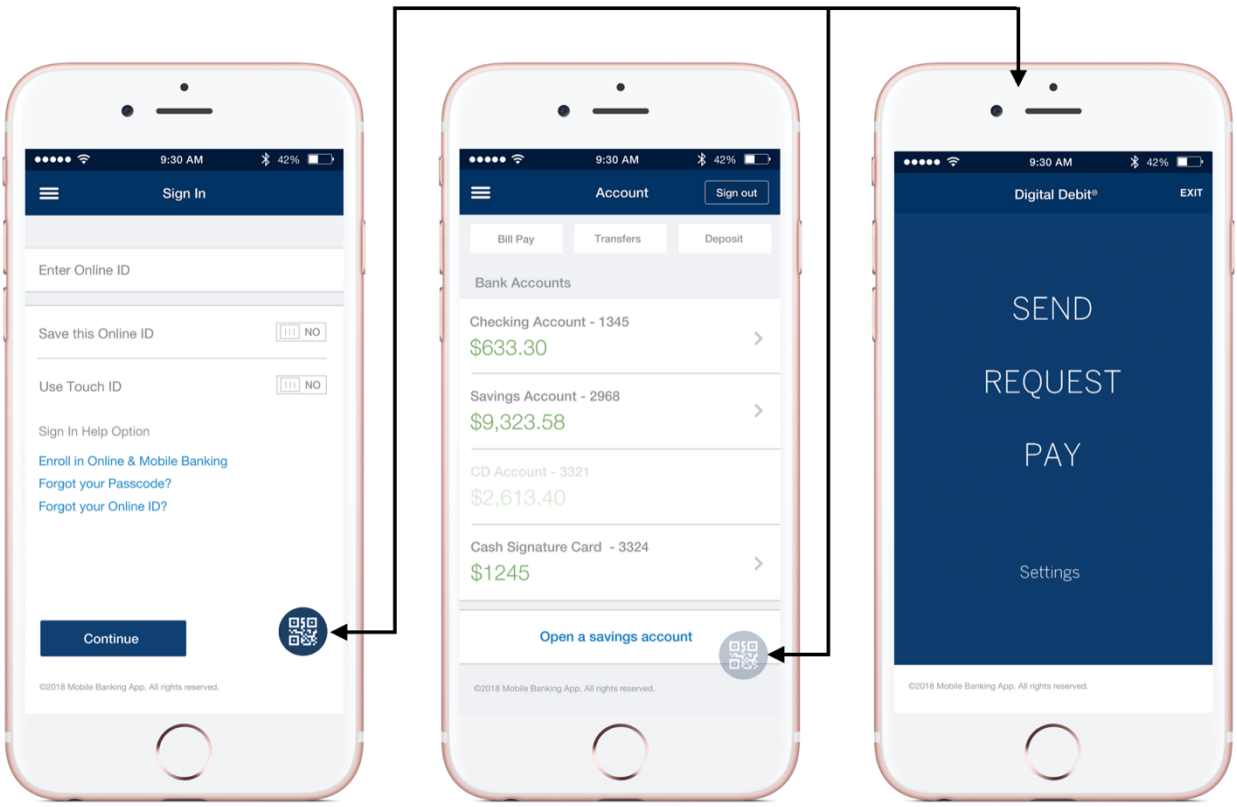
Note: Banks are required to register for a KodeKey token for each ATM and teller station terminal endpoint implementing Digital Debit®.

Digital Debit® ATM Mode should recognize the same ATM PIN code previously assigned to the user's bank account.

Developers can further customize the PIN entry panel with biometric PIN-saving options such as Face ID and Touch ID.



5 Look and Feel



The Digital Debit® panel should be embedded within the look and feel of the host app.

The QR panel banner should include the registered trademark text: Digital Debit®

The Digital Debit® panel shall be accessible from the “Sign In” and “Account” panels as a hover button (provided at the time of license) at the following transparencies:

1) Sign In Panel – 100% full opaque
2) Account Panel – 33% opaque

6 Business Logic

When the user opens the “Digital Debit®” panel from the “Sign In” panel, the user must enter their ATM PIN and use the “Digital Debit®” panel in Quick Pay mode, limiting all transactions to $50 per day. Users can sign in to the full application to use the “Digital Debit®” panel for Full Pay mode, limiting all transactions to the account default set activity limit. Users should be asked permission to activate Digital Debit within the host App and asked to enter their account PIN when using Quick Pay mode from the “Sign In” panel.