ICBA Bancard

Tokenization Enablement

FIS North America Retail Payments

Empowering
the Financial World

Part I
Tokenization Overview

FIS North America Retail Payments

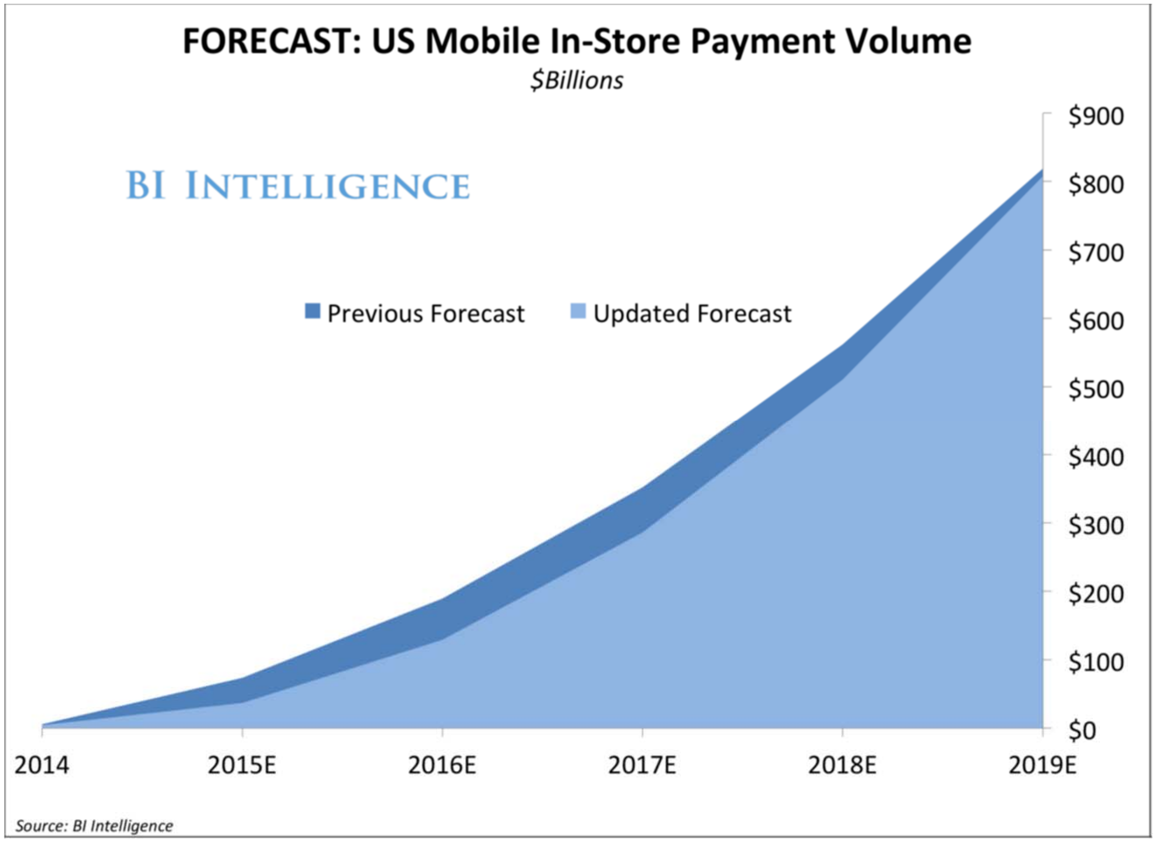
Agenda

- Tokenization Introduction
- Tokenization Transaction Processing
- Tokenization Provisioning with OTP
- Token Residency

Tokenization Intro

- **What is Tokenization?**

Tokenization is the replacement of a card number, or PAN (Primary Account Number), with a pseudo number called a “token,” for use in a digital-payment transaction. Tokenization was introduced to provide an additional layer of defense against fraud by allowing the token to be stored and used in the merchant environment in place of a PAN. This technology is being utilized in today’s many Mobile Wallets including, but not limited to Apple Pay, Samsung Pay, and Android Pay.



Source: http://www.businessinsider.com/the-mobile-payments-report-2015-5

Tokenization Intro

23% ***used an APP for the 1st time in 2015 to buy something***

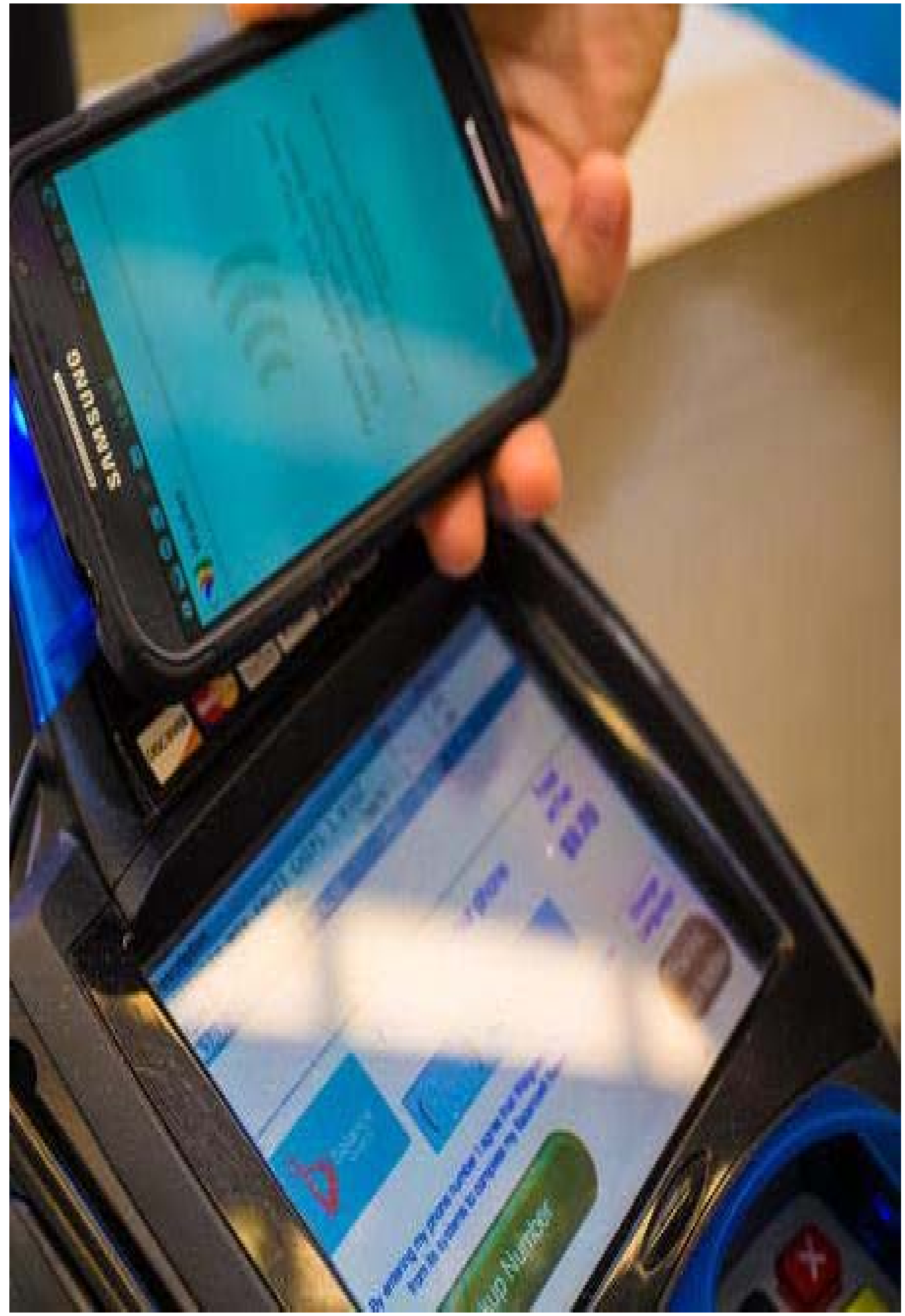
12% ***of consumers used an APP to order a Car Ride***

11% ***of consumers used an APP to make a restaurant reservation***

8% ***of consumers used an APP to book airfare***

- **In 2015, Online Holiday Sales surged to $83 Billion – largely fueled by Mobile**
- **In All, 56% of consumers have used a mobile app for payments**
- ***Total mobile payment transactions are expected to reach $27.05 billion in 2016, with users spending an average of $721.47 annually***

http://www.digitaltransactions.net/news/story/Consumers-Quickly-Embracing-Mobile-Apps-for-Purchases-and-Banking_-Verizon-Study-Finds



Consumer Demand for Apple Pay Outpaces Merchant Acceptance

The Numbers:

- 80 million iPhones in the U.S. , 18% of them are iPhone 6 or 6S , 15% have used Apple Pay at least once, 85% use Apple Pay every time they can

Consumer & Merchant Feedback:

- 59% ask to make a purchase with Apple Pay
- 58% thought it was safer than a normal credit card
- 67% encountered some type of problem such as longer timeframe, unknowledgeable sales person or malfunctioning NFC reader
- 47% went to a retailer that should have accepted the service, but found the service was not yet ready

Tokenization Intro

Continued…

Apple Pay

Cardholders Require Apple iPhone 6, iPhone 6s, iPhone 6 Plus, or iPhone 6s Plus.

Merchants Require Apple Pay Terminal

Samsung Pay

Cardholders Require Samsung Galaxy S7, Galaxy S7 Edge, Galaxy Note5, Galaxy S6 Edge, Galaxy S6 Edge+, Galaxy S6 and Galaxy S6 Active.

Can be used at over 90% of existing merchant terminals using Magnetic Secure Transmission

Android Pay

Cardholders Require any NFC-enabled device running Android OS 4.4 (KitKat) or higher.

Merchants Require Android Pay Terminal

FIS's One Time Passcode Readiness by Platform

OTP Enterprise Step Up Authentication - Platform readiness

#	Milestones to be met	BD	NB	NOR	STP	B2K / TBS		PPS
						Low Est	High Est	
Commit ID	BD is Enterprise BRD	CODAV000135'	CODAV000138	CODAV000140	CODAV000139	JELEW000007	JELEW000007	
	Program Manager	Marci Schoenberger						
Project ID	Proj Mgr	Trevin Larkin	Marie Brattebo	Andy Lind		John Braun		
Business Analyst	Business Analyst assigned to platform dev	Pam Carr-Johnson	Bill Bartlett	Kathleen Scrushy	Celia Goldstein	Barbara Andersen	Tracy Strickland	
	Delivery Projection Date	6/26/2016	9/18/2016	7/31/2016	7/31/2016	7/16/2016	7/16/2016	
	OTP BIN ROUTER	7/16/2016						

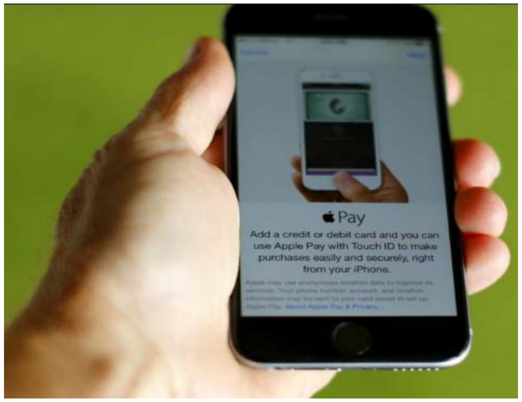
Type equation here.

Tokenization of Mobile Wallets

Consumer Experience

Step One

Provisioning the account number into the mobile device with six digit one time pass code



Step Two

Once mobile device is authenticated the device is ready to submit a payment at NFC terminals

(Samsung can also submit payments at Magstripe POS terminals)

Tokenization Provisioning with OTP

Visa and MasterCard each mandated enhanced step-up authentication with OTP as an additional fraud protection for the provisioning of a mobile wallets (Apple Pay, Samsung Pay and Android Pay) by the account holder to assure Identification and Verification (ID&V) secures the account number in the mobile device. Android Pay also requires a form of step-up authentication above and beyond call center services.

FIS OTP Solution

Visa/Master Card mandates either a six-digit OTP or app-to-app authentication for all 3rd party HCE wallet providers above and beyond call center authentication. FIS will leverage OnDot and Application Programming Interface (API) service integration with Visa/Master Card to deliver the OTP to the end consumer whenever step-up authentication is necessary.

The FIS enterprise OTP solution will be consistent across all FIS card platforms. Each of the FIS card platforms will adopt the FIS enterprise architecture and support the capture of cardholder-level data (i.e., mobile phone numbers and email addresses for each account holder), with an API call that is used to push out a one-time passcode to the cardholder through the “message method” they choose, so that the cardholder can complete the authentication and enrollment processes.

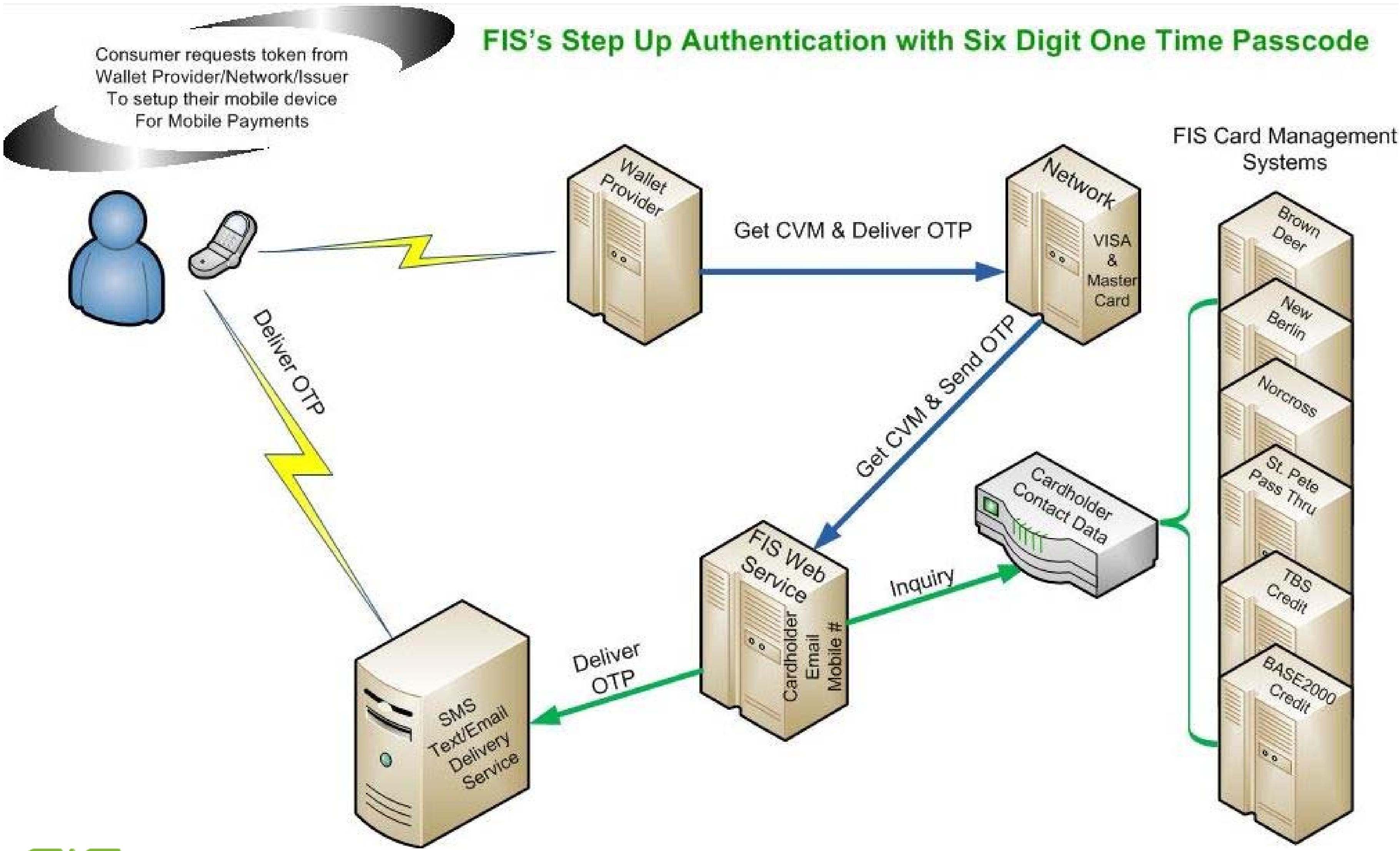
Tokenization Provisioning with OTP

- **How does FIS Tokenization process the step up authentication with six digit one time passcode (OTP)?**

To help meet this requirement, FIS will introduce our enterprise OTP solution, which supports secure delivery of a six-digit, one-time passcode to their cardholder using their mobile phone number and email address on file within the FIS card management systems. We believe that this is the most seamless experience to not only secure the mobile wallet provisioning process, but also ensure a seamless experience for your cardholders.

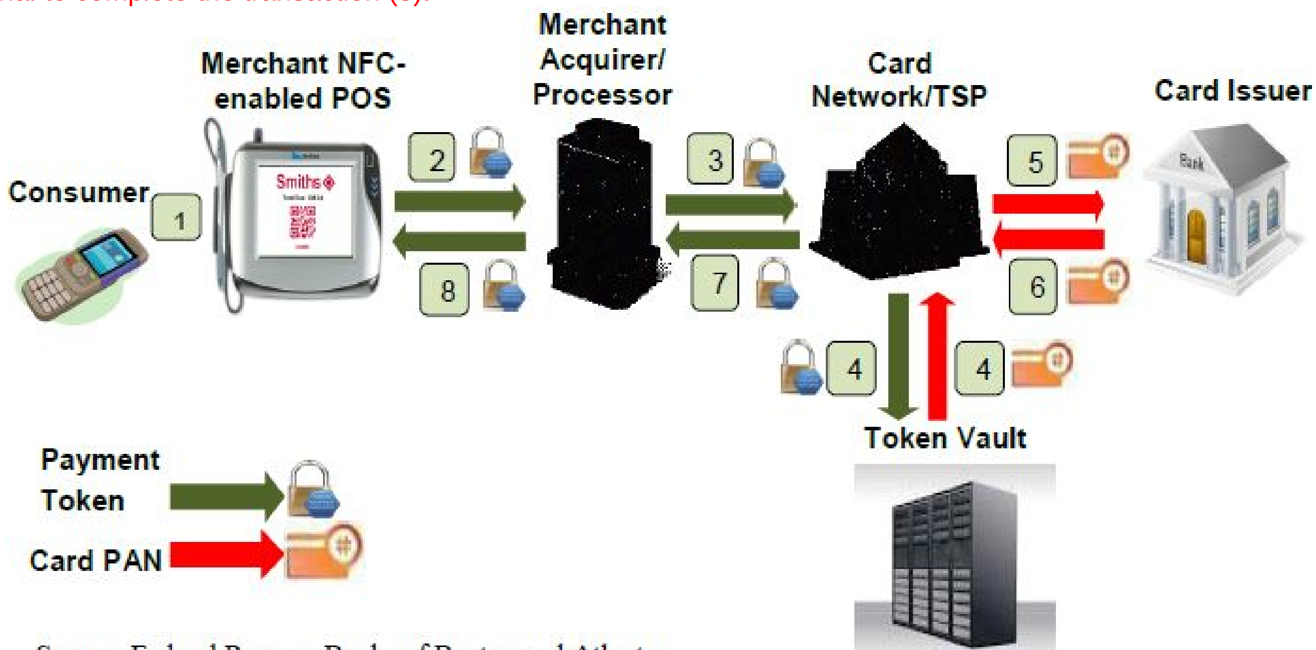
The OTP functionality will be supported through the integration of the application, which will deliver the six-digit OTP value to the cardholder as a part of FIS tokenization services.

FIS's One Time Passcode – "How" it happens



Tokenization Transactions

- **How does Tokenization process the digital-payment transaction?** To make a purchase at the merchant point of sale (POS) terminal, the customer uses their mobile device, which has been preloaded with a payment token stored in the secure element for Apple Pay or in the Host Card Emulation (HCE) in the Cloud for Samsung Pay and Android Pay. The customer uses a fingerprint or passcode on his mobile device to authenticate himself and authorize the transaction to the terminal and verify the purchase amount (1). The POS terminal transmits the payment token, cryptogram and encrypted transaction data to the Merchant Acquirer/Processor (Processor) (2). The Processor sends the payment token, cryptogram and encrypted transaction data to the associated Card Network/TSP [i.e. Visa® / MasterCard®] (3). The Card Network accesses the token vault to map the token and de-tokenize the PAN(4). The Card Network then sends the PAN from the token vault to the Card Issuer for authorization (5). The card Issuer's processor returns its authorization decision to the card network (6). The card network then transmits the payment token and authorization decision back to the Merchant/Acquirer Processor (7). The Merchant/Acquirer Processor sends the authorization decision to the POS Terminal to complete the transaction (8).



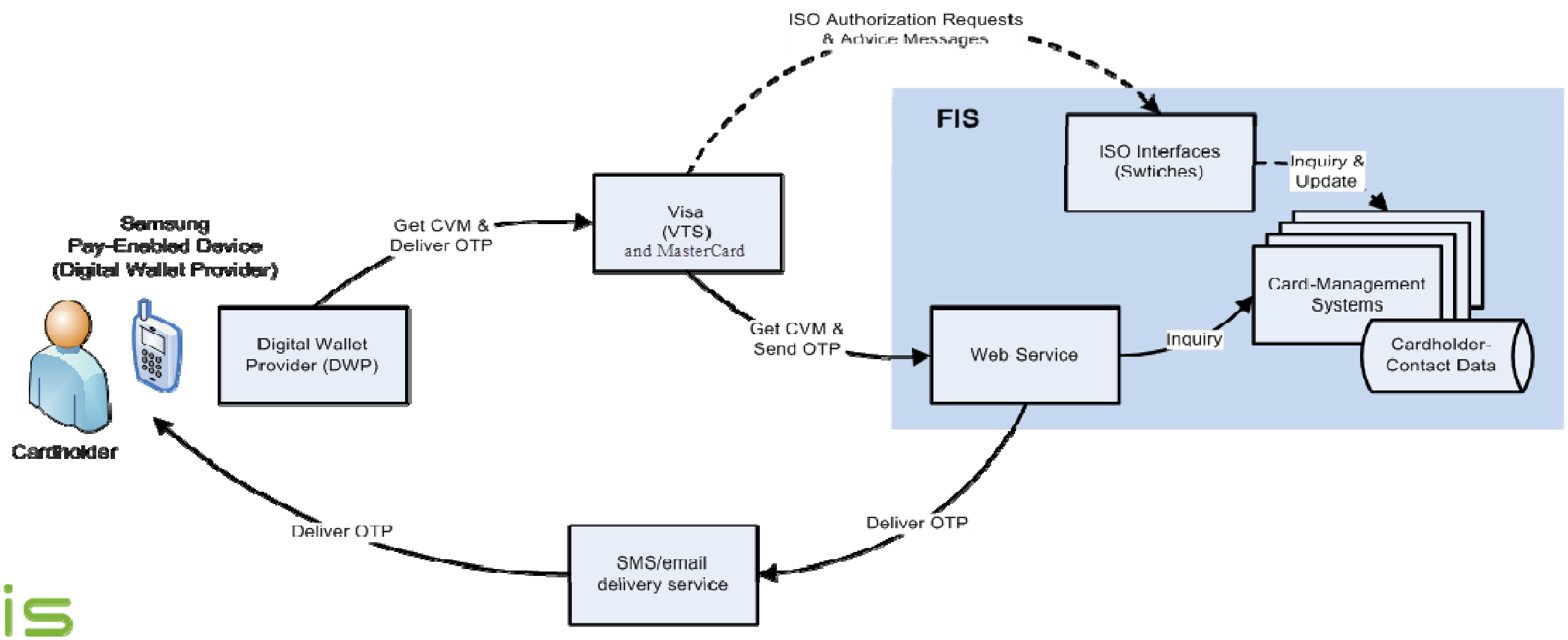
Source: Federal Reserve Banks of Boston and Atlanta

Tokenization Provisioning with OTP

- **How does FIS Tokenization process the step up authentication with six digit one time passcode (OTP)?**

To help meet this requirement, FIS will introduce our enterprise OTP solution, which supports secure delivery of a six-digit, one-time passcode to their cardholder using their mobile phone number and email address on file within the FIS card management systems. We believe that this is the most seamless experience to not only secure the mobile wallet provisioning process, but also ensure a seamless experience for your cardholders.

The OTP functionality will be supported through the integration of the Ondot application, which will deliver the six-digit OTP value to the cardholder as a part of FIS tokenization services.



Tokenization Provisioning with OTP Pricing

Important Note: Each participating institution is encouraged to begin preparation now for the Enhanced *One Time Passcode* step-up authentication solution.

FIS strongly encourages issuers to focus on this data sourcing exercise and ensure that mobile phone numbers and email addresses are in place within our debit and credit systems.

This effort will assure a seamless provisioning experience for your cardholders. In the event mobile phone numbers and email addresses are not on file, the default "call center support service" will be invoked to complete the additional authentication needed to activate the token in the mobile wallet.

Token Residency

- **Is a new token created for every card number, merchant, or transaction?**

Tokens are created for each mobile device as a card is entered, and the token(s) stay static on that mobile device for Apple Pay or in the Host Card Emulation Cloud provided by other wallet providers.

- **After acquiring a token, does the token reside on the mobile device?**

Yes, for Apple Pay only. Not, however, for Samsung Pay, Android Pay or any HCE device.

- **Regarding residency, is there a limit on the number of tokens per card?**

Yes, each token provider will have a maximum number of tokens that can be issued per card. MasterCard will allow up to nine tokens per card. Visa will allow up to 99 tokens per card.

- **Does the issuer own the token?**

Based on the processing platform (credit, debit, prepaid), the financial institution will get to view the tokens provisioned for their cards. The provisioned tokens are created based off of a live Bank Identification Number (BIN) with Visa or MasterCard. Visa and MasterCard are the owners of the BIN and the token. The issuers will not own the tokens provided by Visa and MasterCard.

Part II
Implementation

FIS North America Retail Payments

Empowering
the Financial World

Agenda

- **What is needed from your institution?**
- **What you can expect from FIS?**
- **Mobile Wallet Mass Enablement Timeline**
- **Estimated Go-Live Dates**
- **Recently asked questions**

What is needed from your institution?

- **Complete Enrollment Forms/ Card Art Submitted per Welcome Email**
  - Completed forms including production card numbers to allow for the network to validate the card art set up
  - Card Art and Logo are requirements from Wallet Provider to build the app. FIS will provide to clients a Best Practices document with the size and color requirements.
  - Please take this time to develop your launch strategy and marketing materials. You will later receive instructions on accessing these materials.
  - You will be notified by FIS when to validate the card art. **Please read the communications you receive from us**; they will provide status and, if necessary, any actions that you may need to take.
  - ICBA Bancard & FIS highly encourage webinar attendance. Please register and attend scheduled webinars to aid with your questions. The webinar schedule is communicated in all of our emails to you.
  - If you have questions, email ICBAInquiries@fisglobal.com

What is expected from FIS?

- FIS will manage your Mobile Wallet installs with the Wallet providers and the networks.
- FIS will send you weekly emails that will provide status and updates on your install.
- FIS will monitor the ICBAInquiries@fisglobal.com and ICBAInstall@fisglobal.com mailboxes daily and will provide a response as quickly as possible.
- FIS will be conducting Webinars on the 1st and 3rd Monday; 2nd and 4th Wednesday of each month. These webinars are where you can receive additional information, get your questions answered and hear questions from other clients.

Mobile Wallet Token Enablement Timeline

What to expect next

- **Queue Assignment (*week 0*)**
  - Clients will be placed in Project Queue on *first come, first serve* basis after complete Enrollment Docs are received at ICBAInstall@fisglobal.com. Further instructions will be sent in a Welcome Email from FIS
  - FIS is limited by network bandwidth to *25 Enrollments per week*.

- **Quality Assurance (*week 1*)**
  - Completed forms and Artwork must be provided at the same time
  - Incomplete information will be sent back
  - Artwork – FIS employs a graphic designer who will review and make minor adjustments as needed

- **Implementation Phase (*week 2*)**
  - FIS begins
  - Artwork and metadata will be submitted by FIS to the networks
  - Wallet Providers and the networks begin their build

- **Networks provide confirmation of receipt of paperwork (*week 3*)**
  - Contact your network's respective Web Portal to access Marketing Materials

Mobile Wallet Token Enablement Timeline
(cont.)

- **Card Art Validation Phase (*weeks 3-4*)**
  - FIS will notify you when your test cards are whitelisted for testing purposes
  - You will add your cards to your Mobile Wallets and validate that the Card Art and Card Description load properly

- **Approval Forms to FIS/ Networks (*week 5*)**
  - Visa/MasterCard provide to Wallet Providers the Approval Forms. Visa/MasterCard will communicate when this is complete. An Approval Form will need to be submitted for each Mobile Wallet
  - FIS will receive confirmation from the network that Approval Forms have reached their respective destinations. FIS will update the client

- **Networks and Wallet Providers Approve Launch Dates (*week 6*)**
  - FIS will provide update to the client

- **The project is complete (*week 7*) Full launch occurs for all Mobile Wallets – Your roll out strategy and marketing is occurring.**

Estimated Go Live Dates

Dates indicated below are guidelines. The Wallet Providers and the Networks have tasks that are not in FIS' control and may impact the go-live date.

FI Mobile Data to FIS	FI Mobile Wallet Data to Network	Estimated Date of Production Validation	Approval Form due to FIS	Estimated Apple Response (only applies to Apple)	Target Date with Mobile Wallet (Tuesday)
21-Jun	28-Jun	12-Jul	18-Jul	26-Jul	8/2/2016
5-Jul	12-Jul	26-Jul	1-Aug	9-Aug	8/16/2016
19-Jul	26-Jul	9-Aug	15-Aug	30-Aug	9/6/2016
9-Aug	16-Aug	30-Aug	5-Sep	13-Sep	9/20/2016
23-Aug	30-Aug	13-Sep	19-Sep	27-Sep	10/4/2016
6-Sep	13-Sep	27-Sep	3-Oct	11-Oct	10/18/2016
20-Sep	27-Sep	11-Oct	17-Oct	25-Oct	11/1/2016
27-Sep	4-Oct	18-Oct	31-Oct	8-Nov	11/15/2016
25-Oct	1-Nov	15-Nov	21-Nov	29-Nov	12/6/2016
8-Nov	15-Nov	29-Nov	5-Dec	13-Dec	12/20/2016
22-Nov	29-Nov	13-Dec	19-Dec	27-Dec	1/3/2017
6-Dec	13-Dec	27-Dec	2-Jan	10-Jan	1/17/2017

Recently Asked Questions

What is the Token Bulk Enrollment Form?

One of the most frequently asked questions received concerns the Token Bulk Enrollment form.
This form only pertains to Visa issuers, so if you are a MasterCard issuer, this is a form that you will not need to complete.

a. Why is it needed?

As part of the enrollment process into Mobile Wallets, FIS will provide Call Center Services to manage the validation/authentication of your cardholders prior to their being able to use the Mobile Wallet product on their devices

Visa requires 1-2 people in your organization to have the same access as the FIS Call Center Analysts to support your clients in case FIS needs to refer them to your organization in the event that they cannot be authenticated. You will have the same capability to authenticate and activate a token in the LCM tool.

b. What is VOL?

VisaOnline ,or VOL, is VISA's online portal granting issuers access to necessary network tools (such as LCM and VTR).

c. What is LCM/VTR?

Lifecycle Management (LCM) and Visa Token Reporting (VTR) are services within

Visa Online. The Token Life-cycle Management (LCM) tool is an online tool to help manage life-cycle events of Payment Tokens issued for a Primary Account Number (PAN). This guide is intended to assist the customer service representatives (CSRs) of issuers and their processors in the handling of consumer inquiries that initiate life-cycle updates for Payment Tokens.

The LCM tool allows users to perform a variety of token inquiries and updates as described below:

- Search for one or more tokens and associated information for a PAN
- View token transactions
- Delete/suspend/resume tokens if the consumer's mobile device is lost, misplaced, or found.

VISA Token Reporting (VTR) is a web-based tool that provides access to reports used to manage an issuer's Visa Token portfolio. These reports are generated on behalf of (OBO) the clients by VISA, to capture Apple Pay (or Tokenized) transactions and other details. VISA only provides VTR to Issuers and not Processors. There are a variety of historical reports that may be of interest to you. Visa Token Reporting Services (VTRS) reports show the status of an issuer's tokens, such as provisioning request and declines, authorizations, fraud reporting, and provisioning requests sent to the Yellow Flow.

d. How do I know what my VOL ID is?

In order to access the LCM and VTR services, you must have a valid VISA Online (VOL) ID. A VOL ID is required in order to process the Token Bulk Enrollment form. If you do not have a VOL ID, you will need to go to www.visaonline.com and register for one. You do not need to add services during your registration – those will be added once the Token Bulk Enrollment form is submitted to Visa. Once you have completed the registration for a VOL ID and you receive the ID, you can finish completing the Token Bulk Enrollment form.

Recently Asked Questions

- **What is my FIS ID?**

  Your FIS ID is the identification number that is assigned to your institution. You may also know it by your Entity ID or your FIS Corp ID. If you do not know your FIS ID, please contact your Client Services Manager who will be able to provide this information.

- **What do you mean by FIS Issuer Platform?**

  The FIS Issuer Platform is where you process transactions. You could process through the Milwaukee Debit (BCFS), New Berlin (FISA, FISB, and IFSA), Base2000, TBS, Norcross, or St. Pete Pass Thru platform. If you are unsure, please contact your FIS Client Services Manager for more information.

- **What is my BID?**

  Your BID is a Business Identification Number assigned to your organization by Visa. If you do not know this number, please contact your Visa Account Representative or ICBA Bancard for clarification.

Recently Asked Questions

- **What is my ICA and how do I know if I'm a principal member?**

  Your ICA is your Inner Bank Card Association number assigned to your organization by MasterCard. If you do not know your ICA # or whether or not you're a principal member, please contact your MasterCard Account Representative or ICBA Bancard.

- **Are business cards eligible?**

  Small business cards are eligible, but corporate business cards are not. At this time, commercial cards are not able to meet Identification and Verification requirements since, by nature, they do not belong to an individual.

- **What are RGB Values?**

  The RGB Values we request on the *Tokenization Setup Form* refer to the general colors of the card background and font graphics (Red, Green, Blue). White, for example, is denoted (255,255,255) and black is denoted (000,000,000). These colors will show in place of the card image on the app should an error occur while loading the image.

Recently Asked Questions

- **How do I enter more than one Short Description since I have 2 cards?**

First to explain the short description – it is just a description of the BIN. For example, you may have a platinum debit bin, a rewards debit bin and a standard debit bin. The short description will inform your Cardholders which card they have enrolled in the Mobile Wallet. Please refer to the Tokenization Setup form example #1 for a visual on how the short description is displayed. The Short description is the verbiage contained in the parenthesis in the example. Unfortunately the Tokenization Setup Form has a character limitation in the Short Description field. While it's true that Apple, Samsung, and Android have a 32 character limit for the short description, our form does not allow you to add more than one short description. If you do have multiple BINs that are using different short descriptions, please provide the short description and corresponding BIN in the body of your email when you send the completed forms back to us.

- **Can we use custom Terms and Conditions?**

FIS will provide standard verbiage that will be used for the cardholder Terms and Conditions text that will appear. Here is the verbiage that will be provided:

> *"The storage and usage of your payment card number (and credentials corresponding to your payment card number) in this digital wallet are subject to the terms and conditions of the applicable cardholder agreement with your payment card issuer, as in effect from time to time. Please contact your payment card issuer for more information."*

- **Is there a due date for the forms to be returned back to you?**

There is not a specific due date for the completion of the forms. Once you submit all of the required documentation outlined in the welcome email to the ICBAInstall mailbox, you will be placed into the implementation queue. All implementations will commence on a first-come, first-serve basis. As previously mentioned, you will receive status emails throughout the Implementation Process. ICBA Bancard is only funding this project through 2017, so any major delays should be avoided.

Recently Asked Questions

- **What does the Card Validation testing cover?**

  Card art validation will entail adding the test cards provided on your Tokenization Setup Form to each Mobile Wallet (Apple Pay, Samsung Pay, and Android Pay) using the appropriate devices to ensure the card images appear appropriately. *No transaction testing will occur at this time*. Only after you approve of the loads, Card Art, etc. will we move forward.

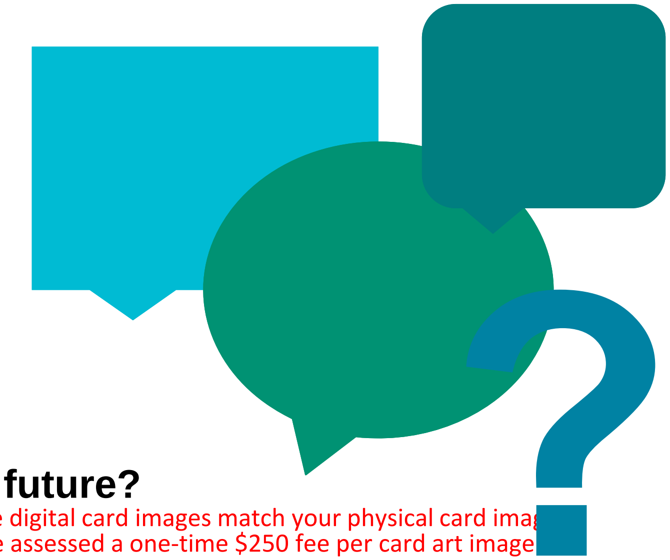
- **Why do we need to provide our PIN Network(s) on the Setup Form?**

  Mobile Wallet transactions can be conducted using either signatures or PINs. After the enrollment process completes with the token vault owners (Visa or MasterCard), we can facilitate the enrollment of your PIN network as well. For credit card issuers, if you allow your credit BIN to conduct PIN based transactions, then you will need to list your most predominant PIN Network (for example, NYCE, STAR, PULSE, etc.). Please note, as we can facilitate the enrollment of your PIN network, we are also dependent on the certification of your PIN network. You should contact your account representative at those PIN networks to determine their certification status.

- **How many Card Images do you require/ allow?**

  We require one card image per *BIN type*. For example, if you currently have 3 different types of credit cards – say a Platinum, Rewards and Classic Card –all may have a different image. During this project, however, you may only upload *one image* for all Credit BINs. The same holds true if you have a Debit BIN and/or an HSA BIN. If you have both Credit and Debit BINs, you may upload two Card Images- one for Credit and one for Debit.

Recently Asked Questions



- **Will customized Card Art be available at the BIN level in the future?**

  Yes. After you go live with your Mobile Wallets, if you are interested in changing your card art so that the digital card images match your physical card imag you may contact your FIS Customer Service Representative and open a project at FIS to do so. You will be assessed a one-time $250 fee per card art image change.

- **Why do you require Test Cards and how should they be setup?**

  To complete the previously mentioned *Card Art Validation,* you will need to provide on your Tokenization Setup Form LIVE/ACTIVE/VALID cards free of any holds in your production system belonging to valid accounts. Typically, institutions provide FIS with Card information belonging to staff at the FI. We will need both cards belonging to an eligible Apple device owner and cards belonging to eligible Samsung devices owners (which may also be used for Android Pay Testing).

- **What is required to enroll Prepaid and H.S.A BINs?**

  Prepaid and HSA BINs are eligible to enroll in Mobile Wallets. However, there are additional steps that are necessary before they become part of the enrollment process. Each network has different requirements regarding these BIN types. For a **MasterCard** issuer, HSA programs with product codes MHA and MHH are supported. If you have any other type of HSA program, they are ineligible. If you have questions regarding the type of BIN you currently have, it is best that you reach out to your MC Account Rep. If you do know that your HSA BIN has product codes MHA and MHH, you do not need to do anything other than list the BIN on the set up form and provide the card image and test card information.

  If you are a **VISA** issuer, Visa requires approval of the Prepaid or HSA BIN prior to enrolling it into Mobile Wallets. If you have a Prepaid or HSA BIN, you would list it on the FIS Set up form as well as provide the card image and test card. During the QA review, our analyst will send you the Visa Prepaid/HSA approval form that Visa requires. You will fill out the form and send it directly to Visa. Once you receive the approval, you will send the approved form back to FIS so that we can submit it to Visa with all of your enrollment materials. Visa will not move forward in the enrollment until they have a copy of the approved form.

Recently Asked Questions

- **When will we be able to test?**

The testing dates are provided on the Estimated Go Live Dates slide – slide #7. You will also receive email communications from your FIS analysts that will alert you to your testing schedule and inform you of the testing requirements.

- **What are the FI Approval Forms?**

The FI Approval Forms are specific to each Mobile Wallet and serve as your agreement that you are ready to launch your Card Products in the respective Wallet. Once you have reviewed that your Card Art images load correctly and you are comfortable with moving forward, you will supply FIS with the completed forms via the ICBAComplete mailbox, which will then be forwarded to your network(s).

- **What reports will FIS provide?**

FIS will provide a report specific to the Token Provisioning. It will be provided by processing platform. This report is based on advice received by the networks, and will have specific delivery methods and format based on the network and the platform. If you are looking for any other report, you would need to reach out to your specific network via their location/services in their Online Portals.

Recently Asked Questions

- **Are there specific SLAs on the mandated Customer Notification?**

  None of the Mobile Wallet Providers have specified SLAs or enforced any specific content in the notifications. It has been left up to the issuer to establish these SLAs and delivery method type (email vs. paper mail). If requested, the FIS Implementation Team can provide a sample letter that can be adapted by the institution. For more information on this requirement or to receive such a template, please request at ICBAInquiries@fisglobal.com.

- **What marketing information is available for us from the Mobile Wallet Providers or my network?**

  Each network has specific marketing requirements. As part of the enrollment process, FIS will provide you instructions on how to obtain your marketing materials per network. The marketing materials are all available online via your respective network. You will receive an email communication after the network has accepted your submission and prior to your card art validation phase with further instructions on how to access these materials.

Recently Asked Questions

- **Will FIS provide tokenization customer support if you are not currently providing customer support for other products?**

  Yes, use of the FIS Call Center is *required* for issuers going through the Mass Enablement activity. This will include the tokenization support for enrollment, authentication and other token related questions.

- **Can you explain the FIS Enterprise call center hours of operation?**

  We set the hours of operation for the call center to be the best timeframes to support Tokenization and Tokenization calls based on research. The hours will be reviewed on a periodic basis to determine the best way to service customers. The hours of operation for the FIS Enterprise Call Center (subject to change) are Monday through Sunday, **8:30 a.m.** to **11:00 p.m. ET.**

- **If the institution has a call center and does not use FIS for any of these services, will the institution be able to have access to the Visa/MasterCard tools for activation and troubleshooting?**

  No, all activation and troubleshooting calls for tokenization will go through the FIS call center.

Questions?

Thank You for participating in
ICBA Bancard
Tokenization Enablement

Empowering
the Financial World