ERCOT IT Forum
Road map for retail market system changes

ERCOT Public
February 23, 2018

Agenda

Part 1

- Retail Application Health Assessment

Part 2

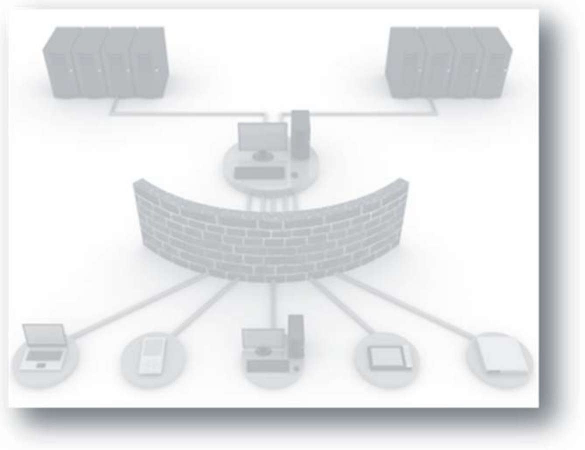
- URL changes to the Market Operations Test Environment (MOTE) and Retail Market Test Environment (RMTE, formerly CERT)
- Infrastructure upgrades in MOTE/RMTE and Production environments
- New Secure Socket Layer (SSL) certificates in MOTE/RMTE and Production environments
- New Intermediate and Root Certificate Authority (CA) certificates
- Security updates for API communication

Retail Application Health Assessment

February 2018

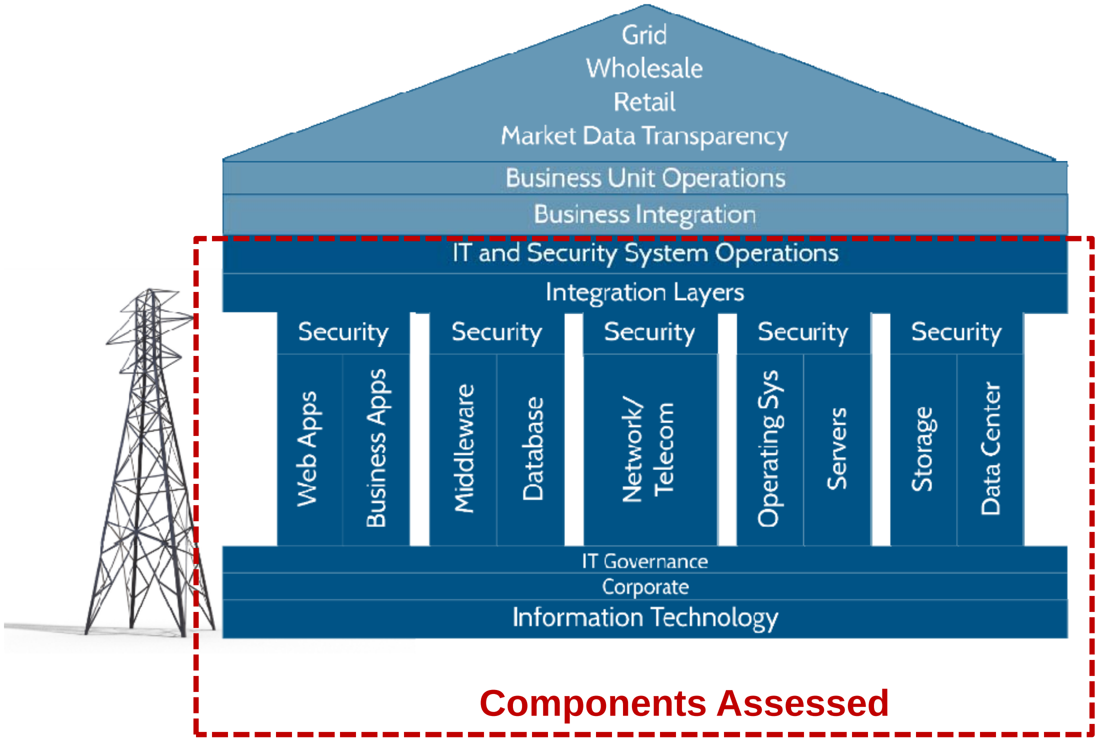
Version 4.1.9

Public



Core Technology and Methodology

Overview of Platform Assessment Methodology



- The Platform health forecast incorporates assumed upgrades in all in-progress projects as well as within project concepts currently under consideration
- The underlying platforms of each Business Application are assessed against both the vendor and ERCOT established roadmaps
- The life-cycle phase of each component is assigned a color code and numeric score to represent the component's overall health status

– Supported version	Green (5)
Consider upgrade	Yellow (3)
Upgrade required	Red (1)

Retail

Retail Stakeholders

Business Area	Systems	Dev Manager	IT Ops Manager	Primary Business Owner	Business Owner
Retail	Data Transport (NAESB) EDI MarkeTrak FlighTrak DataTrak (DTR) Siebel	McDonald	Pagliai	Ruane	Michelsen

Strategy:

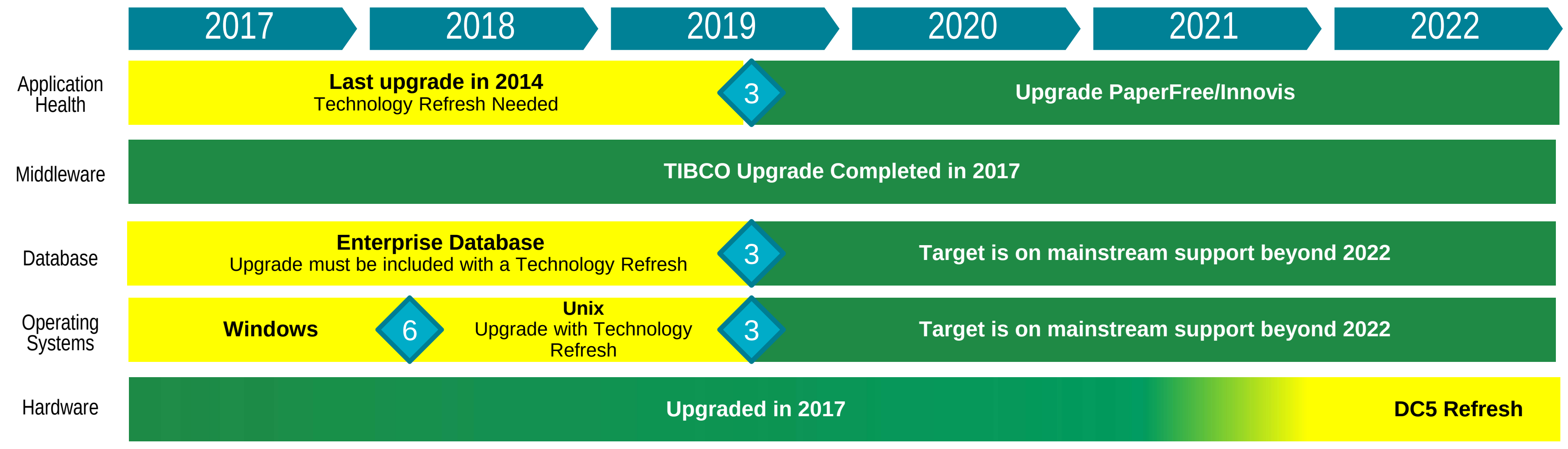
Update Products for Usability

- Upgrade supporting retail systems to vendor-supported versions
- Improve retail market participant end user portal with a focus on reliability, resiliency and usability
- Evaluate additional integration options based on performance and stability of more current standards.
- Upgrade Innovis application and supporting applications per vendor roadmap
- Redesign FlighTrak for Market Participant Flight Certification
- Upgrade any platforms on vendor extended support contracts

	Project	Project Source	Target End Date
1	Enterprise Database Upgrade	PPL	2019
2	Siebel Upgrade	Concept	2019
3	Innovis Application Suite Upgrade	PPL	2019
4	Serena (MarkeTrak) Upgrade	PPL	2017
5	DTR Tech Refresh	Concept	2019
6	Retail Windows Upgrade	PPL	2018
7	EDI Replacement	PPL	2019
8	ERCOT Flight Certification	PPL	2019

Data Transport (NAESB)

Main gateway to receive and send Retail Choice transactions. Provides secure, reliable and non-repudiation form of communication between Market participants.



2017 | 2018 | 2019 | 2020 | 2021 | 2022

Application Health: **Last upgrade in 2014** Technology Refresh Needed — 3 — **Upgrade PaperFree/Innovis**

Middleware: **TIBCO Upgrade Completed in 2017**

Database: **Enterprise Database** Upgrade must be included with a Technology Refresh — 3 — **Target is on mainstream support beyond 2022**

Operating Systems: **Windows** — 6 — **Unix** Upgrade with Technology Refresh — 3 — **Target is on mainstream support beyond 2022**

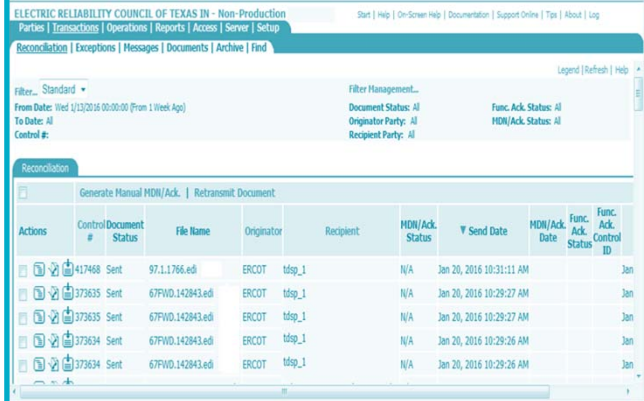
Hardware: **Upgraded in 2017** — **DC5 Refresh**

Key Information:

3 Innovis Application Suite Upgrade will be needed to replace aging technology stack. Complete technical stack refresh to include the application, database, and Unix upgrades

6 Retail Windows servers replaced in early 2018

- TIBCO upgrade completed in 2017



ELECTRIC RELIABILITY COUNCIL OF TEXAS IN - Non-Production

Start | Help | On-Screen Help | Documentation | Support Online | Tips | About | Log
Parties | Transactions | Operations | Reports | Access | Server | Setup
Reconciliation | Exceptions | Messages | Documents | Archive | Find
Legend | Refresh | Help
Filter Management...
Reconciliation
Generate Manual MDN/Ack. | Retransmit Document

Filter... Standard

From Date: Wed 1/13/2016 00:00:00 (From 1 Week Ago)
To Date: All
Control #:

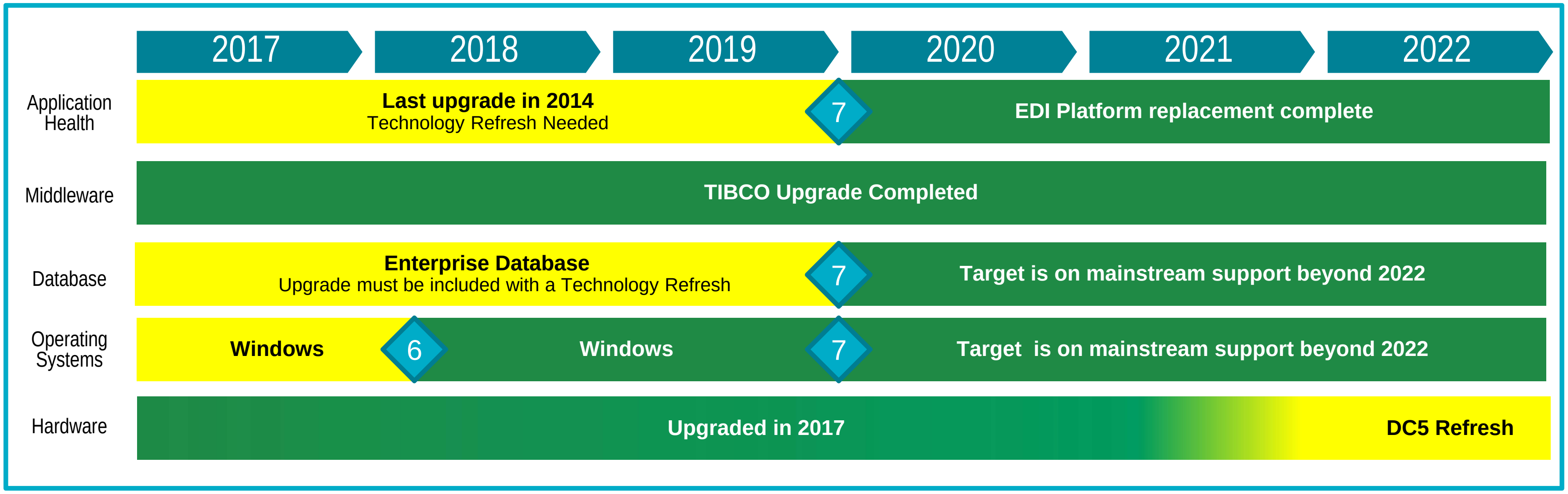
Document Status: All
Originator Party: All
Recipient Party: All

Func. Ack. Status: All
MDN/Ack. Status: All

Actions	Control #	Document Status	File Name	Originator	Recipient	MDN/Ack. Status	▼ Send Date	MDN/Ack. Date	Func. Ack. Status	Func. Ack. Control ID	
□	417468	Sent	97.1.1766.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:31:11 AM				Jan
□	373635	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:27 AM				Jan
□	373635	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:27 AM				Jan
□	373634	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:26 AM				Jan
□	373634	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:26 AM				Jan

Electronic Data Processing (EDI)

EDI system is responsible for enforcing ANSI and TXSET rules. This system acquires, translates, validates, packages and formats transactions in support of Retail Customer Choice and generates functional acknowledgement.

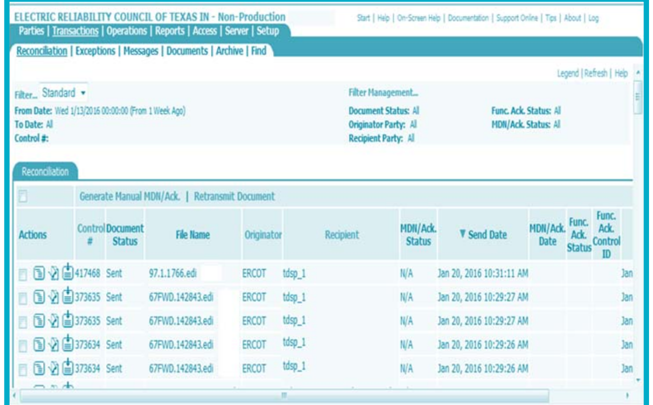

2017
2018
2019
2020
2021
2022
Application Health
Last upgrade in 2014
Technology Refresh Needed
7
EDI Platform replacement complete
Middleware
TIBCO Upgrade Completed
Database
Enterprise Database
Upgrade must be included with a Technology Refresh
7
Target is on mainstream support beyond 2022
Operating Systems
Windows
6
Windows
7
Target is on mainstream support beyond 2022
Hardware
Upgraded in 2017
DC5 Refresh

Key Information:

7 EDI Replacement Assessment project is targeted complete in 2Q 2018 with a recommendation of the product selection. The replacement product is assumed to implement at the end of 2019.

6 Retail Windows servers replaced in early 2018

- TIBCO upgrade completed in 2017



ELECTRIC RELIABILITY COUNCIL OF TEXAS IN - Non-Production

Start | Help | On-Screen Help | Documentation | Support Online | Tips | About | Log
Parties | Transactions | Operations | Reports | Access | Server | Setup
Reconciliation | Exceptions | Messages | Documents | Archive | Find
Legend | Refresh | Help

Filter... Standard ▾

From Date: Wed 1/13/2016 00:00:00 (From 1 Week Ago)
To Date: All
Control #:

Filter Management...

Document Status: All
Originator Party: All
Recipient Party: All

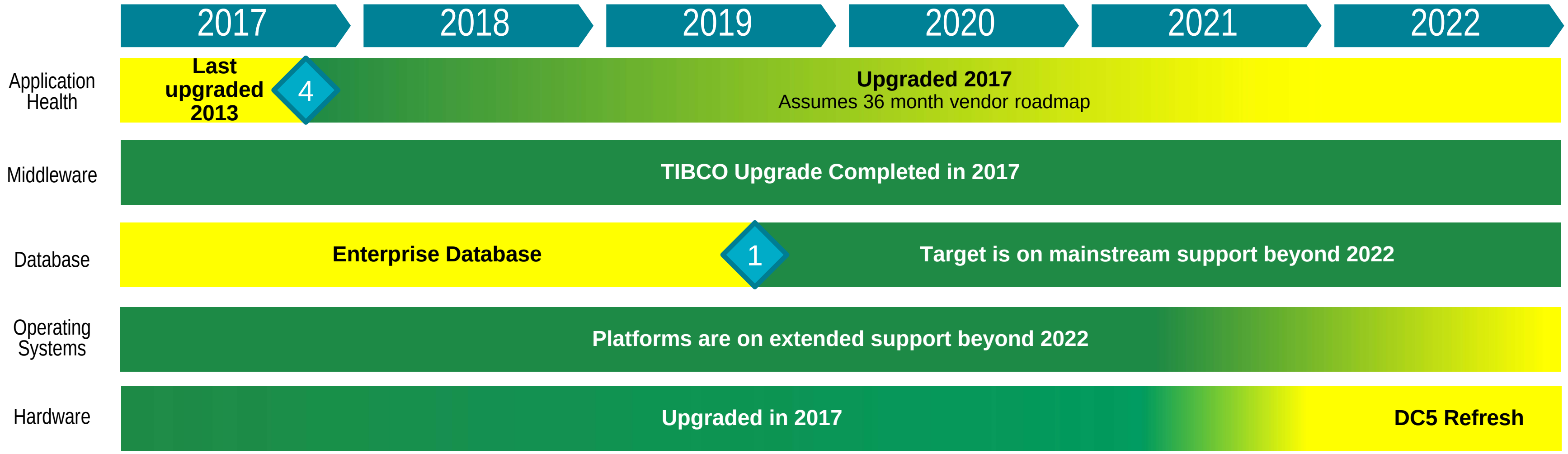
Func. Ack. Status: All
MDN/Ack. Status: All

Reconciliation
Generate Manual MDN/Ack. | Retransmit Document

Actions	Control #	Document Status	File Name	Originator	Recipient	MDN/Ack. Status	▼ Send Date	MDN/Ack. Date	Func. Ack. Status	Func. Ack. Control ID	
□	417468	Sent	97.1.1766.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:31:11 AM				Jan
□	373635	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:27 AM				Jan
□	373635	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:27 AM				Jan
□	373634	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:26 AM				Jan
□	373634	Sent	67FWD.142843.edi	ERCOT	tdsp_1	N/A	Jan 20, 2016 10:29:26 AM				Jan

MarkeTrak

MarkeTrak tracks and resolves retail market issues and data discrepancies. Issue types include: Missing Transactions, Usage/Billing, Rejected Transactions, Rep of Record, Cancel, Inadvertent Gain/Loss, Customer Rescission, Switch Hold Removal, Safety Net Order and Service Disconnect.



	2017	2018	2019	2020	2021	2022
Application Health	**Last upgraded 2013** 4 **Upgraded 2017** Assumes 36 month vendor roadmap					
Middleware	**TIBCO Upgrade Completed in 2017**					
Database	**Enterprise Database** 1 **Target is on mainstream support beyond 2022**					
Operating Systems	**Platforms are on extended support beyond 2022**					
Hardware	**Upgraded in 2017** **DC5 Refresh**					

Key Information:

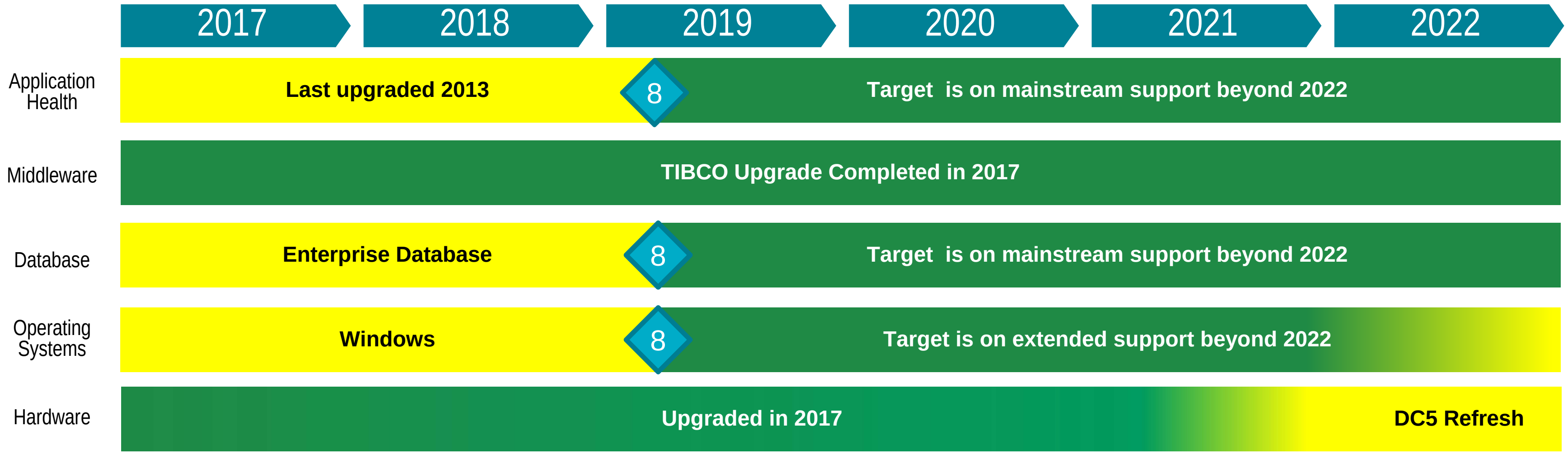
4 MarkeTrak base product (TeamTrack) upgraded in 2017

1 The Enterprise Database requires a minor version upgrade for long term support

- Tibco components upgraded with MarkeTrak upgrade

FlighTrak

FlighTrak is an external web interface utilized for executing mandated ERCOT certification of retail Market Participants (etod.ercot.com).



2017 2018 2019 2020 2021 2022

Application Health: Last upgraded 2013 — 8 — Target is on mainstream support beyond 2022

Middleware: TIBCO Upgrade Completed in 2017

Database: Enterprise Database — 8 — Target is on mainstream support beyond 2022

Operating Systems: Windows — 8 — Target is on extended support beyond 2022

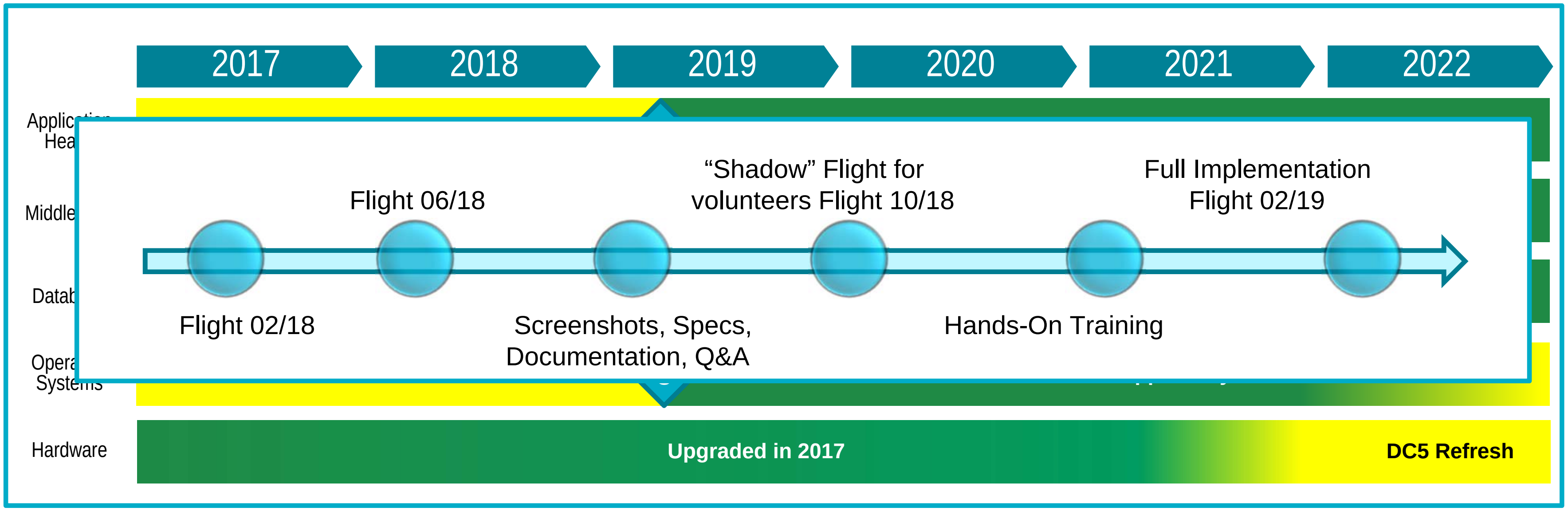
Hardware: Upgraded in 2017 — DC5 Refresh

Key Information:

- 8 FlighTrak upgrade project refreshes the technology for the certification interface to meet current browser and security requirements for implementation in February 2019
- The upgrade also increases visibility for the ERCOT certification process for new LSEs entering the Retail market and existing LSE changing system parameters.
- Multifactor authentication solution is to be determined

FlighTrak

FlighTrak is an external web interface utilized for executing Protocol mandated ERCOT certification of retail Market Participants (etod.ercot.com).



Flight 02/18

Flight 06/18

Screenshots, Specs, Documentation, Q&A

"Shadow" Flight for volunteers Flight 10/18

Hands-On Training

Full Implementation Flight 02/19

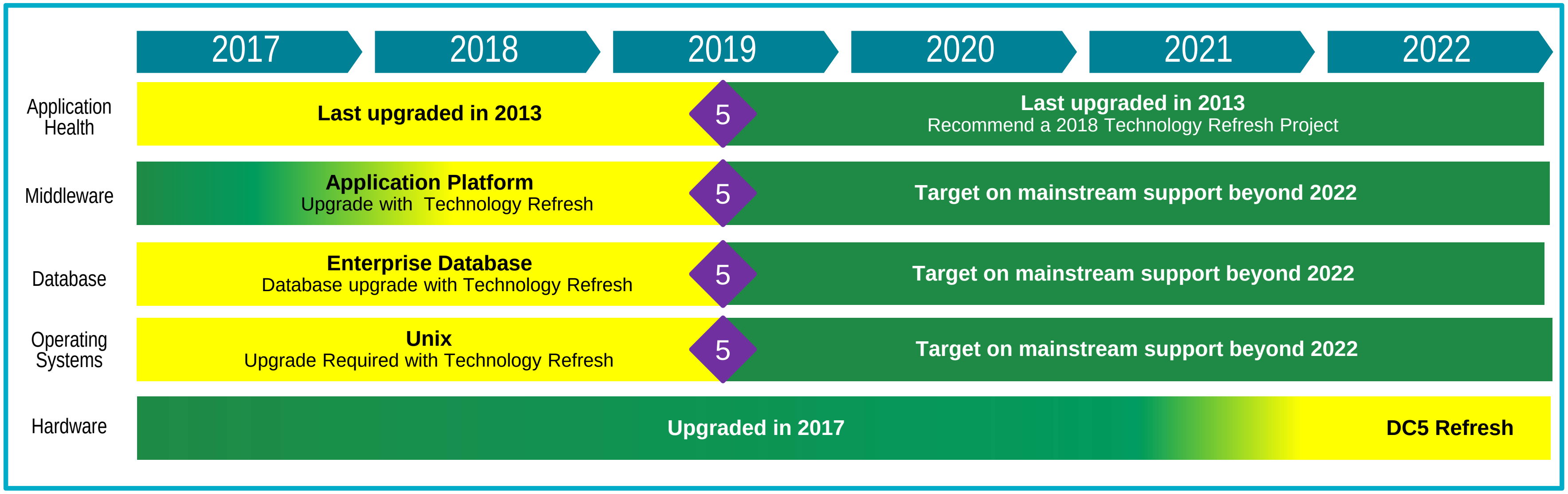
Key Information:

8 FlighTrak upgrade project refreshes the technology for the certification interface to meet current browser and security requirements for implementation in February 2019

- The upgrade also increases visibility for the ERCOT certification process for new LSEs entering the Retail market and existing LSE changing system parameters.
- Multifactor authentication solution is to be determined

DataTrak (DTR)

DTR is an internal-only, ERCOT developed application. It provides multi-system processing visibility, reporting of Retail Market Transaction processing times, and enables PUCT Market Metrics reporting. DataTrak enables the Retail Choice business team to monitor retail transaction processing and address exceptions occurrence



2017 2018 2019 2020 2021 2022

Application Health: **Last upgraded in 2013** | 5 | **Last upgraded in 2013** Recommend a 2018 Technology Refresh Project

Middleware: **Application Platform** Upgrade with Technology Refresh | 5 | **Target on mainstream support beyond 2022**

Database: **Enterprise Database** Database upgrade with Technology Refresh | 5 | **Target on mainstream support beyond 2022**

Operating Systems: **Unix** Upgrade Required with Technology Refresh | 5 | **Target on mainstream support beyond 2022**

Hardware: **Upgraded in 2017** | **DC5 Refresh**

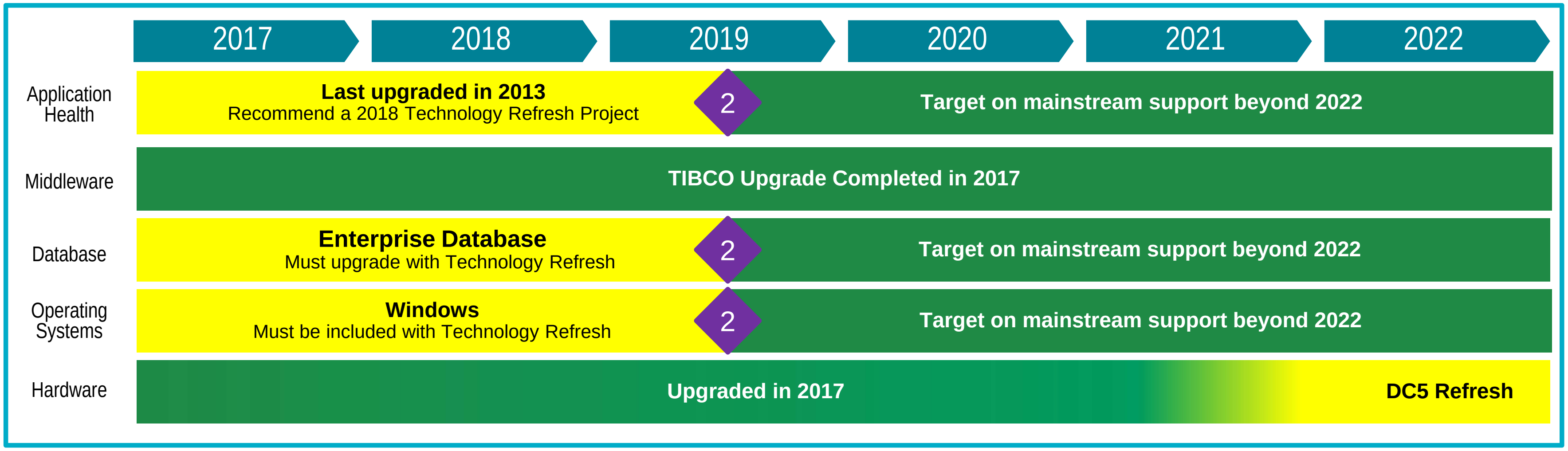
Key Information:

5 Recommend a Technology Refresh project to ensure long term support of the DTR product

- Upgrade server platform for maximum support lifecycle
- Include the Java platform as part of Technology refresh
- Include upgrading the enterprise database as part of Technology refresh
- Upgrade will be tied to EDI Replacement Project

Registration and Transaction Processing (Siebel)

Official system of record for Retail and Wholesale Registration, Dispute and Service Request management system that includes Market Registration, Market Participant and Resource Registration, Service Requests, Settlement Disputes and Retail ESIID Registration/Transaction Processing: Service Accounts, Service Orders, Service instances


2017
2018
2019
2020
2021
2022
Application Health
Last upgraded in 2013
Recommend a 2018 Technology Refresh Project
2
Target on mainstream support beyond 2022
Middleware
TIBCO Upgrade Completed in 2017
Database
Enterprise Database
Must upgrade with Technology Refresh
2
Target on mainstream support beyond 2022
Operating Systems
Windows
Must be included with Technology Refresh
2
Target on mainstream support beyond 2022
Hardware
Upgraded in 2017
DC5 Refresh

Key Information:

2 Initiate Siebel Technology Refresh for completion in 2019 to upgrade core application to a current Innovation pack to address technology components upgrades in product suite

- The TIBCO integration product upgrade was completed early 2017

IT to IT Forum

Leo Angele

ERCOT IT

ERCOT Public
February 23, 2018

Agenda

- URL changes to the Market Operations Test Environment (MOTE) and Retail Market Test Environment (RMTE, formerly CERT)
- Infrastructure upgrades in MOTE/RMTE and Production environments
- New Secure Socket Layer (SSL) certificates in MOTE/RMTE and Production environments
- New Intermediate and Root Certificate Authority (CA) certificates
- Security updates for API communication

Introduction

This presentation will answer the following questions:

- Who is affected by these changes?
- Why is ERCOT changing URLs in MOTE/RMTE?
- Why is ERCOT upgrading Secure Socket Layer (SSL) Certificates?
- What is changing in relation to API Security?
- What is the timeline for the Upgrade?
- What do Market Participants need to do to prepare?
- What steps do Market Participants need to take for API access?
- What are the risks of not preparing prior to the upgrade?
- Where do Market Participants find all of ERCOT’s SSL and Client Digital Certificate Root CAs?

Target Audience

Who is affected by these changes?

- Users utilizing the Market Operations Test Environment (MOTE) and Retail Market Test Environment (RMTE, formerly CERT) User Interfaces (UI)
- All Application Programmatic Interfaces (API's) connecting to ERCOT environments for ERCOT's External Web Services (EWS), including submissions and Get List/Report functionality, and access to the MarkeTrak API

Why Change URLs?

Why is ERCOT changing URLs in MOTE/RMTE?

- testing.ercot.com was originally created as a sandbox environment for the Nodal market implementation
- ERCOT is standardizing test URLs
- Current URLs:
  - (UI) https://testing.ercot.com
  - (API) https://testingapi.ercot.com
  - (WAN API) https://testingapi.wan.ercot.com
- NEW URLs:
  - (UI) https://testmis.ercot.com
  - (API) https://testmisapi.ercot.com
  - (WAN API) https://testapi.wan.ercot.com

Why Upgrade?

Why is ERCOT upgrading SSL Certificates?

- Due to DigiCert purchasing Symantec’s SSL certificate division, all SSL certificates must be issued using the new DigiCert Intermediate and Root CAs
- ERCOT’s current MIS.ERCOT.COM SSL certificate expires on April 23, 2018 and will be replaced on April 11, 2018
- MISAPI.ERCOT.COM and API.WAN.ERCOT.COM SSL certificates will be replaced on April 18, 2018

What API Security Changes?

What is changing in relation to API security?

- ERCOT has identified a configuration issue that is causing the system to not validate that API communication is being submitted with a valid ERCOT issued Client Digital Certificate at the handshake level
- ERCOT will implement the configuration change to ensure that API communication is being sent with a handshake level valid ERCOT issued Client Digital Certificate as well as having each message signed with a valid ERCOT issued Client Digital Certificate
- Market Participants that are not currently submitting API communication with a valid ERCOT issued Client Digital Certificate will see a disruption in service if not corrected

Timeline

What is the timeline for the Upgrade?

- ERCOT's new MOTE/RMTE URLs will be configured on March 7, 2018 to facilitate Market Participant testing
- ERCOT is providing five weeks of testing in MOTE to ensure all Market Participants have adequate time to prepare for the production migration
- ERCOT's Production Market Information System (MIS.ERCOT.COM) secure website will be configured with a new DigiCert SSL server certificate on April 11, 2018
- ERCOT's Production External Web Services (MISAPI.ERCOT.COM/ API.WAN.ERCOT.COM) secure websites will be configured with new DigiCert SSL server certificates on April 18, 2018
- All API's connecting to ERCOT's Production External Web Services will need to have the new SSL Root Chain installed in the API keystore and the API security changes in place before the SSL certificate upgrade on April 18, 2018

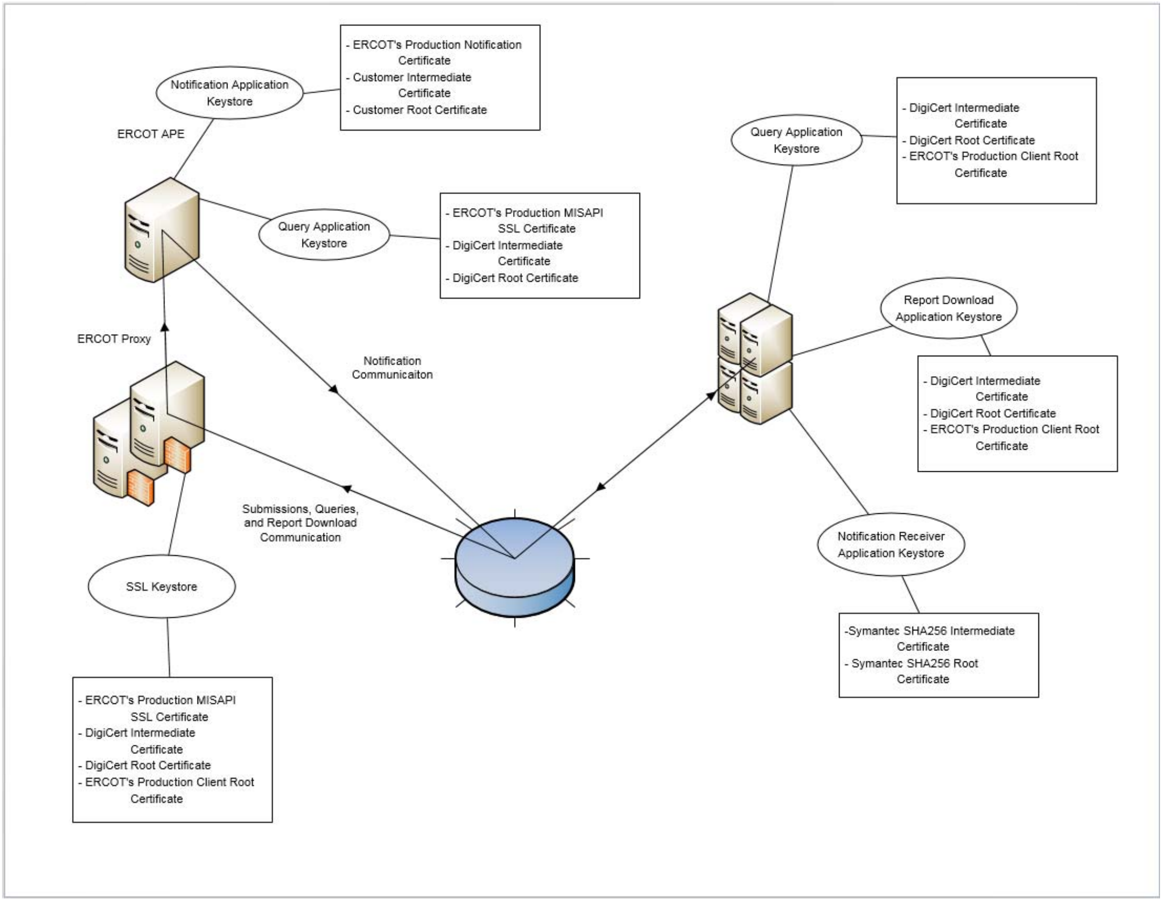
Preparation

What do Market Participants need to do to prepare?

- Market Participants must download the new DigiCert Root and Intermediate Certificates from ERCOT.com prior to the configuration changes
- Market Participants must install the new DigCert Root and Intermediate Certificates into any API keystore that is used to connect to ERCOT's External Web Services prior to the configuration change
- Market Participants should NOT remove the existing Symantec Root and Intermediate Certificates at this time
- The new DigCert Root and Intermediate Certificates will be required for both the Production and MOTE environments
  - ERCOT has provided sample instructions for Market Participants to use as a guide when installing the new DigiCert Root and Intermediate Certificates at the following location:
    - http://www.ercot.com/services/mdt/webservices/index.html
- Ensure that API communication is being sent with a handshake level valid ERCOT issued Client Digital Certificate as well as having each message signed with a valid ERCOT issued Client Digital Certificate

API Keystore

The diagram below explains a typical keystore location and the minimum required certificates.



ERCOT APE

Notification Application Keystore

- ERCOT's Production Notification Certificate
- Customer Intermediate Certificate
- Customer Root Certificate

Query Application Keystore

- ERCOT's Production MISAPI SSL Certificate
- DigiCert Intermediate Certificate
- DigiCert Root Certificate

ERCOT Proxy

SSL Keystore

- ERCOT's Production MISAPI SSL Certificate
- DigiCert Intermediate Certificate
- DigiCert Root Certificate
- ERCOT's Production Client Root Certificate

Notification Communicaiton

Submissions, Queries, and Report Download Communication

Query Application Keystore

- DigiCert Intermediate Certificate
- DigiCert Root Certificate
- ERCOT's Production Client Root Certificate

Report Download Application Keystore

- DigiCert Intermediate Certificate
- DigiCert Root Certificate
- ERCOT's Production Client Root Certificate

Notification Receiver Application Keystore

-Symantec SHA256 Intermediate Certificate
- Symantec SHA256 Root Certificate

Risks

What are the risks of not preparing prior to the described changes?

- Failure to install the new SSL Root Chain in the API keystores before the SSL certificate upgrade will affect the availability of:
  - Programmatic communication
    - External Web Services (EWS)
    - Application Programmatic Interface (API) submissions
    - Get List/Report functionality
  - Access to the MarkeTrak API
- Failure to ensure that API communication is being sent with a handshake level valid ERCOT issued Client Digital Certificate before the SSL certificate upgrade will affect the availability of:
  - Programmatic communication
    - External Web Services (EWS)
    - Application Programmatic Interface (API) submissions
    - Get List/Report functionality
  - Access to the MarkeTrak API

Location of Certificates

Where do Market Participants find all of ERCOT’s SSL Root and Intermediate Certificates?

- ERCOT has published a list of all required SSL and Client Digital Certificate Root CAs on ERCOT.com.
- http://www.ercot.com/services/mdt/webservices/index.html
- Market Participants can contact their Client Services Representative for further questions

Questions and Answers

- Do I have to revoke/reissue all of my user’s Digital Certificates? Will we need to regenerate private certificates and install them along with the root certificates?
  - No, this is just the SSL certificate that secures the API website. No client certificates will be affected.
- Does the USA have to install the SSL certs?
  - No, IT administrators of the MP’s API will need to manually install the SSL Intermediate and Root certificates into the API’s keystore.
- Does this affect everyone?
  - No, only applications currently connecting to ERCOT’s EWS API system and applications receiving ERCOT issued API Notifications.
- As an IMRE type MP, do we need to take any action on this?
  - IMRE’s typically don’t use an API to query/download data and they do not make submissions.
- What needs to be changed on our side? Is it just uploading new cert to our key store and removing old or more than that?
  - The new Root and Intermediate certificates need to be imported into your existing keystore(you do not have to remove the old). If you choose to use a fresh keystore, you must wait until the SSL certificate is installed on ERCOT’s systems prior to switching your system to the new keystore.
- To do testing, do I need a test API cert? If so how do I get it?
  - Yes, you need an API certificate to test the API. Your USA can issue an API certificate for you.
- I tried connecting to MOTE/RMTE but I could not connect. Do I need any certificate to connect to this environment? If so how do I get it?
  - Yes, you need a MOTE certificate to test in the MOTE environment (testmis.ercot.com and testmisapi.ercot.com). Your USA can issue an appropriate user or API certificate for you.

Discussion