

# FedRAMP Cloud - Leveraging a High Environment for Secure Deployment

# Agenda

**I. WHAT WE DO**

**II. XTEC FEDRAMP SERVICE**

**III. XTEC AND THALES**

**IV. DEPLOYMENT THOUGHTS**

# Luna as a Service - Cloud-Based Hardware Security for Government

- Industry-Leading, FedRAMP High Authorized
- Thales Luna T-Series Network HSM Now Available in the Cloud
- **Benefits:**
  - Cloud deployment flexibility
  - Zero upfront costs, pay-as-you-go pricing
  - Focus on your mission, not hardware management
  - High availability included
  - Supports Cloud Smart initiatives

Trusted Cyber Technologies

THALES

## Luna Credential System

### HSM-Secured Identity Credentials

Thales TCT's Luna Credential System introduces a new approach to multi-factor authentication by maintaining user credentials in a centralized hardware device that is securely accessible by endpoints in a distributed network. It unites the familiarity of certificate-based authentication with the security of a FIPS 140-2 certified HSM.

### Public Key Infrastructure Basics



# XTec Corporate Overview



**US Based**



**Industry Focus & Dedication**



**Scope of Services**



**Strong Authentication Focused**

**Qualified**

**Compliant**

**Economical**

## **Incorporation**

Founded in 1992

## **Headquarters**

Miami, Florida

## **Government Initiatives**

Reston, Virginia

**First Central Smart  
Card Issuance  
Solution for the  
Federal Government**

**End-to-End  
Knowledge and  
Solutions**

# XTec Solution Overview



**Purpose Built**



**Security First**



**Infrastructure**



**Performance**



**Authentication**



**Experience**

**Proven**

**Secure**

**Reliable**

## Products

- Enrollment & Issuance Solutions
- Lifecycle Management Solutions
- Authentication Authority
- Physical Access Solutions
- HSM-AAS

## Services

- System Integration Services
- Help Desk Services
- Program Support Staff



# Certifications

- Compliance
  - Certified PIV-I Issuer
  - NIST FIPS 201
  - GSA APL Approved
  - Over 12 C&A's
- FedRAMP High Authorized



Agency	Confidentiality	Integrity	Availability	Overall
BBG	Moderate	Moderate	Moderate	Moderate
U.S. Navy	Moderate	High	Moderate	Moderate
DHS	High	High	High	High
DOL	Moderate	Moderate	Moderate	Moderate
DOS	High	High	High	High
NSF	Moderate	Moderate	Moderate	Moderate
Smithsonian	Low	Low	Low	Low



- **Federal Risk & Authorization Management Program**
- Run by GSA, with DHS & DoD
- Securing the Cloud for Federal Use

**FedRAMP = Cloud Service Provider (CSP)**

+ Security Controls (SP 800-53)

+ Authorization

+ Do Once, Use Many

# FedRAMP and AUTHENTX<sup>TM</sup> CLOUD

## FEDRAMP MARKETPLACE

### FedRAMP at a Glance



READY

23



IN PROCESS

89



AUTHORIZED

296

(as of March 17, 2023)

### Impact Level

24 High

231 Moderate

6 Low

35 Low – SaaS

296 Authorized



2  
Authorizations

Xtec, Incorporated - AuthentX Cloud

FedRAMP Authorized Since 08/02/2019

### System Profile

Service Model  
SaaS

Deployment Model  
Government Community Cloud

Impact Level  
High

### Contact Information

POC: Heather Brooks  
E-mail: [fedramp@xtec.com](mailto:fedramp@xtec.com)  
Website: <http://www.xtec.com>

### FedRAMP Authorization Timeline

04/26/2018  
In-Process

08/02/2019  
Authorized



## Compliance

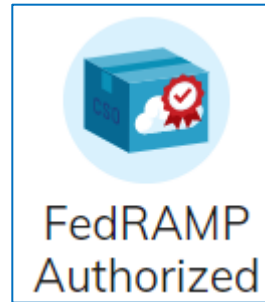
- FedRAMP Authorized
- FIPS 201 Approved
- Approved PIV/PIV-I Issuer
- ISO 21188 (PKI at Financial Organizations)
- Section 508 (Accessibility)

## Continuous Monitoring

57 Controls Continuously Monitored

Including:

- Monthly Vulnerability Scans
- POA&M Flaw Tracking
- Annual 3PAO Assessment



ISO 21188

# AuthentX Cloud Big Picture

## Functionality

- Identity Management
- Credential Management
  - PIV, Derived PIV
  - PIV-I
  - Mobile, Other
- Digital Certificate Services
- Physical Access Control
- Hardware Security Module (HSM) as a Service (HaaS)

### AuthentX Functionality

#### Equipment

Enrollment & Issuance Workstation  
Light Enrollment  
Light Issuance/Activation



#### Lifecycle Management

Self Service Kiosk  
Desktop Application  
Secure Appliance



#### Authentication & Validation

Authentication Authority  
OCSP, CRL, LDAP, PDVAL, SCVP  
FICAM Registration Station

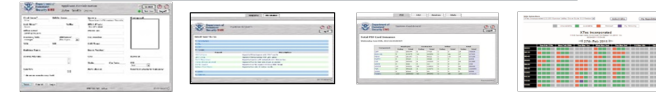


#### Physical Access Control

End-to-End solution  
PIV, PIV-I, CAC  
Permission branches  
Permission assignments  
Reporting  
Monitoring  
Certification Authentication



### AuthentX Web-Based User Interfaces



Workflow

Reporting

Dashboard

Scheduling

+Monitoring, Audit Logs, HelpDesk, Admin

### AuthentX Web Portal



Provisioning & Authentication

### Identity Credentialing



PIV

PIV-I

Temp

FAC

Visitor

Derived

### Enterprise Services

#### PKI Architecture

Federal Bridge- Common Policy  
SSP's, NFI SSP's  
Authentication Authority



#### Data Sharing

Ad-Hoc Reporting Engine  
Standards-based Interfaces  
Automated data population  
Automated data exchange  
One-way near-real-time  
Two-way web services

#### ICAM Enablement

Core Digital Identity Authority  
Automated Provisioning  
Central Authentication  
PACS and LACS Enablement  
Existing PACS automated provision  
Existing LACS directory auto  
provisioning



#### Sustainability

New standard incorporation  
guaranteed: derived, multi-factor,  
biometrics, FIPS 201-2, cardstock,  
admin privileges, etc.

## AuthentX Cloud Customers

### Executive Branch

- US Agency for Global Media
- Department of Energy
- Drug Enforcement Administration
- National Science Foundation



U.S. AGENCY FOR  
GLOBAL MEDIA



### Judicial Branch

- US Courts
- US Court of Appeals for Veterans Claims



### Commercial

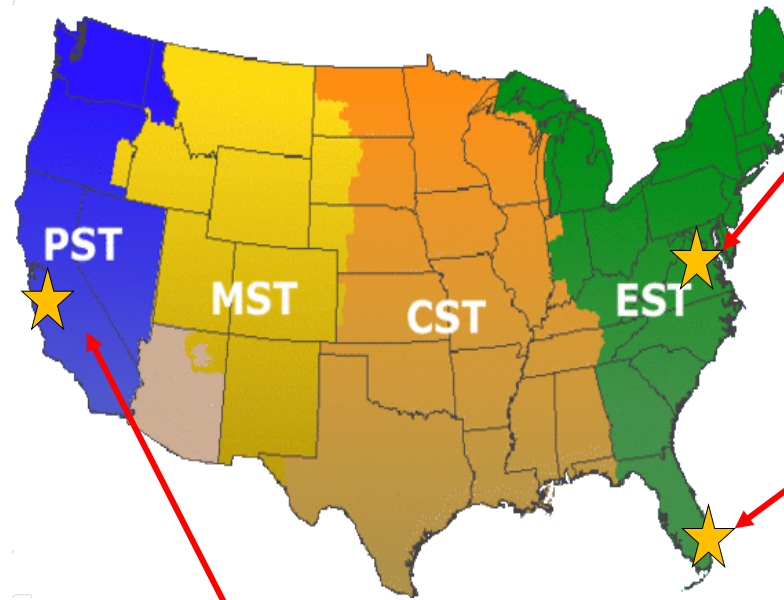
Fiserv organizations requiring **strong authentication** to federal agency systems:

- Dept. of Treasury
- Dept. of Education



## Cloud Hosting

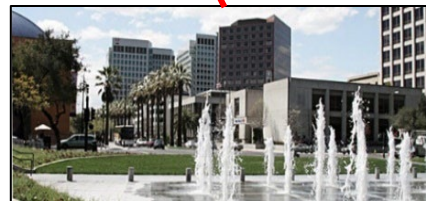
- Equinix Data Centers
- Highly Available
  - 3 Geographically Remote Facilities
  - Data Replication
  - Load Balancing
  - Each Site Serves as a Primary
- Highly Secure
  - XTec Private SCIF (Miami)
  - Secure Cages (Culpeper, Santa Clara)



**NAP of the Capitol Region**  
*Culpeper, VA*



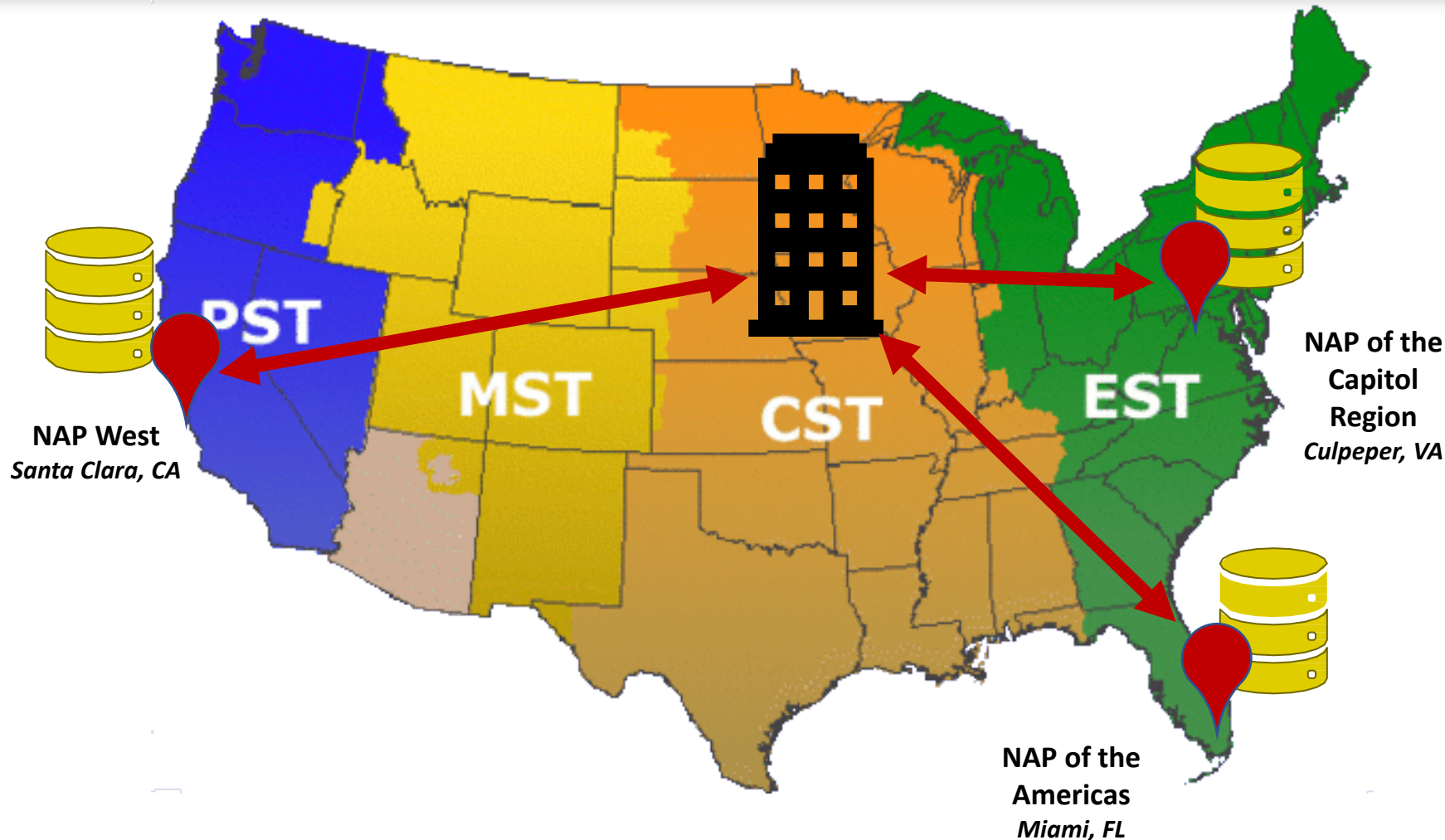
**NAP of the Americas**  
*Miami, FL*



**NAP West**  
*Santa Clara, CA*



# Luna as a Service Architecture



## Dedicated HSM

- Full cryptographic control
- Access to a single appliance hosted at 1 of 3 datacenters.
- High Availability Option
- Add a local Backup HSM for offline storage.

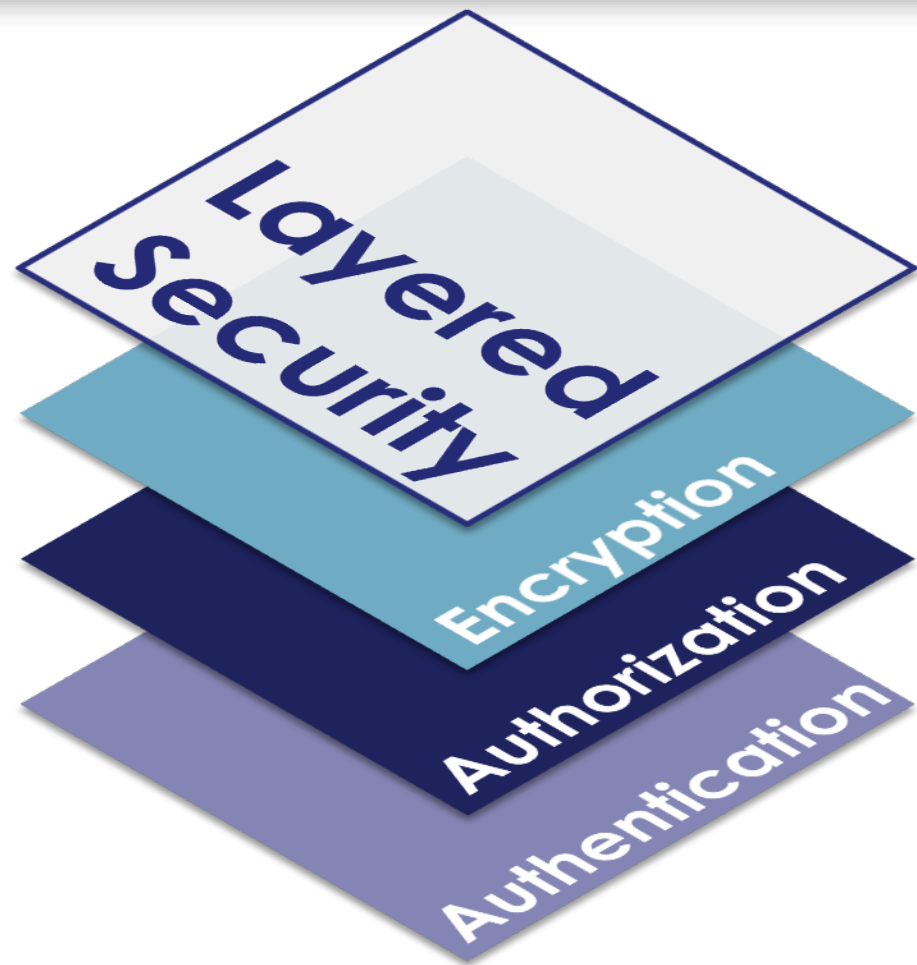
## Managed HSM

- Scalable, cost-effective
- Administrative tasks handled by HSM Engineers.
- Includes High Availability and secure replication across three datacenters.

## Credential System

- Cloud-based multi-factor authentication with FIPS 140-2 Level 3 certified HSM security.

# NTLS Layered Security



## Encryption

- TLS v1.2/1.3 protected sessions
- User-configurable cipher suites

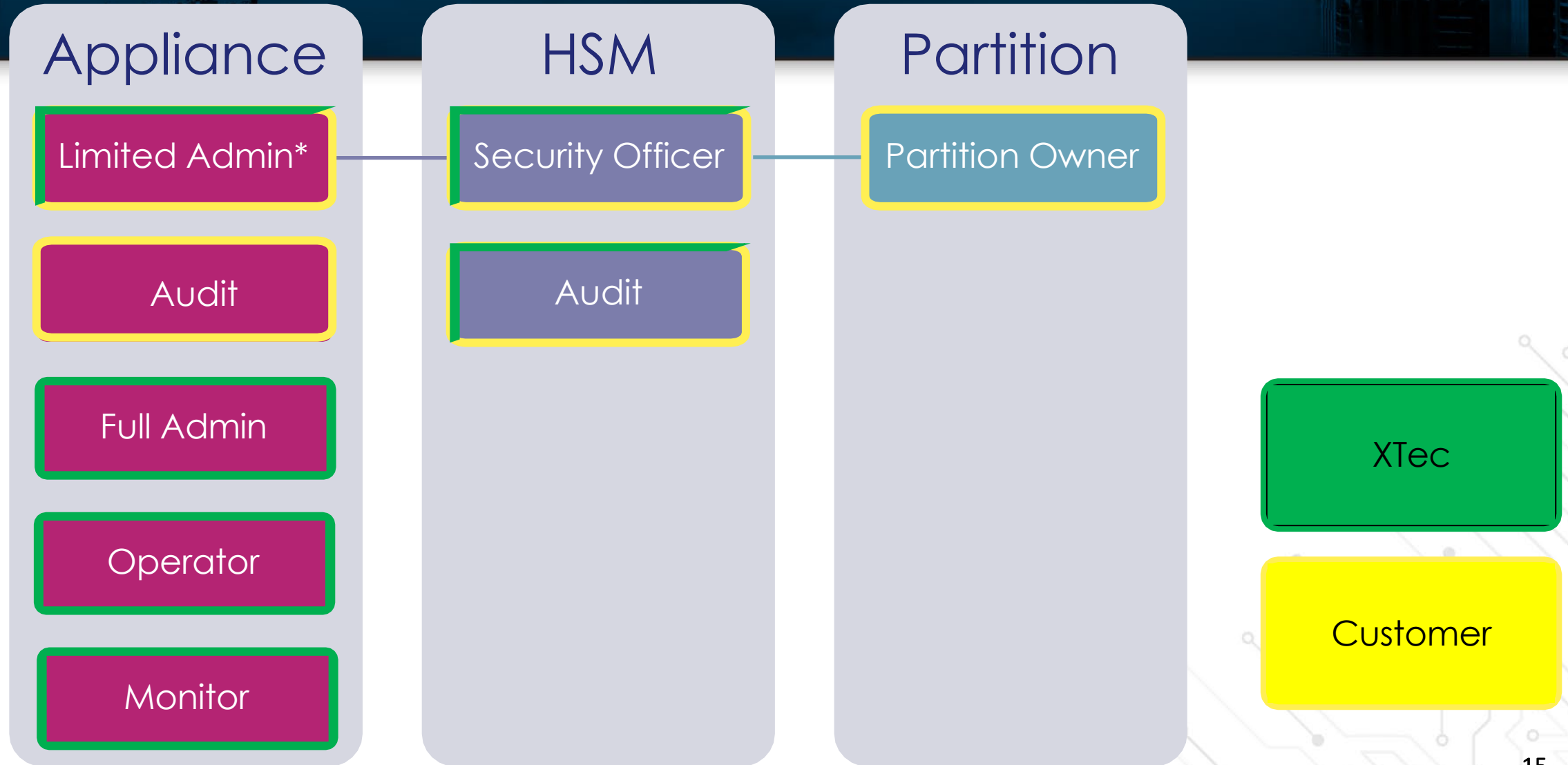
## Authorization

- Clients white-listed by certificate
- IP/DNS check performed
- Assigned to individual partitions

## Authentication

- Clients must provide credentials to access partition objects

# Separation of Roles



# Where can you take this?

## Secure Database

- ❖ Leverage Thales APIs to protect master DB keys using HSM in the Cloud
  - ❖ Strong asymmetric crypto functions in a geographically distributed environment
- ❖ Leverage AuthentX credentialing system to provide smart card and Mobile access to DB resources
  - ❖ Validated solution for a variety of platforms

## HSM Backed Virtual Smartcards

- ❖ An integrated solution that would allow access to the “smart card” from anywhere
  - ❖ Solutions to meet Federal or AATL Policies

## Integrated Signing Solution

- ❖ Remove the limitations of current Adobe Signing
  - ❖ Sign Adobe documents with the end user credential
    - ❖ On desktop
    - ❖ On Mobile



Signed and all signatures are valid.



# Why Thales TCT and AuthentX Cloud

## Security & Compliance

- ❖ FIPS 140-2 Level 3 and CNSS approved
- ❖ FedRAMP High authorized
- ❖ Accelerates adoption of Executive Order 14028 and National Security Memorandum 8 requirements
- ❖ U.S. Based Provider- All employees, data centers and development in the U.S.

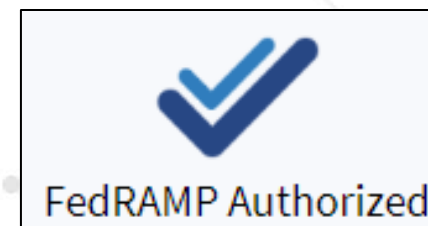
## Flexibility

- ❖ Solution set provides various options
  - ❖ Managed or Dedicated HSMs OR Credential Service
  - ❖ Backup and High Availability options

## Various Integration Points

- ❖ Thales TCT APIs can be leveraged within AuthentX Cloud services
- ❖ Leverage AuthentX interfaces for systems integration

THALES



# Benefits of **AUTHENTX**<sup>TM</sup> CLOUD



Added Security



Convenience



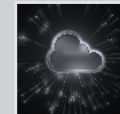
Cost Efficiency



Federal  
Compliance



Continuous  
Monitoring



Enhanced  
Infrastructure



Transparency

# Questions



**Heather Brooks**  
**hbrooks@xtec.com**