



# **NextGen External User Management System (XMS) Overview**










# NextGen XMS – Capabilities

U.S. Department of Health and Human Services

**NextGen XMS is a scalable, cloud-based solution that allows OpDivs to focus on their mission; and takes into consideration:**

- Alignment with Digital Identity guidelines, ICAM and Cloud modernization efforts
- Security and compliance with federal standards ( NIST, OMB, HHS EPLC requirements, etc.)
- Identity and Access Governance and delegated administration model
- Enterprise service that can secure access to external HHS applications
- Centralized platform that is flexible to integrate with third-party providers and services

## Capabilities & Benefits

	<b>Secure Access:</b>	<i>Allows external users to access protected applications using credentials issued by the General Services Administration's (GSA's) Login.gov or via other agency's PIV/CAC</i>
	<b>NIST 800-63-3 Compliance:</b>	<i>IAL1, IAL2, and IAL3, and AAL2 and AAL3</i>
	<b>Identity Proofing/Delegated Proofing:</b>	<i>Remote ID proofing using Login.gov; and delegated proofing for users that affiliate with an organization that's managed within NextGen XMS.</i>
	<b>Organization Affiliation:</b>	<i>Ability to create organizations and manage affiliations to those organizations within NextGen XMS</i>
	<b>Access Requests/Approvals:</b>	<i>Configurable access request framework for an application</i>
	<b>Organization Relationship Management:</b>	<i>Ability to create organizations and manage affiliations to those organizations</i>
	<b>Accredited Platform and Helpdesk:</b>	<i>NextGen ATO in place which includes Login.gov; no impact to integrated application's ATO, only ISA/MOU required</i>



# NextGen External User Management System (XMS) Overview

U.S. Department of Health and Human Services

The Authentication and Access Management services are supported via the NextGen External User Management System (XMS) across the external, non-HHS user community.

## NextGen XMS Services:

- Authentication Services<sup>1</sup>
- Identity, Account, and Entity Management Services<sup>2</sup>
- Data Services<sup>3</sup>

<sup>1</sup> Simplified Sign-On & Federation Capabilities

<sup>2</sup> Application Account and Entity Linking Capabilities

<sup>3</sup> Reporting and Auditing Capabilities

HHS.gov | EXTERNAL USER MANAGEMENT SYSTEM U.S. Department of Health and Human Services

Select a Login Method

Login PIV or CAC Login

**LOGIN.GOV**

The External User Management System (XMS) is using a credential provider to allow you to sign in to your account safely and securely.

If you do not have an existing Login.gov account, you will be able to create one before you log in.

**LOGIN**

? Help i HHS Privacy Policy i Privacy Act Statement



In alignment with NIST 800-63-3 guidelines, NextGen XMS offers:

## Identity Assurance Levels

### IAL 1

**Little or no confidence in asserted identity**

No requirement to link the applicant to a specific real-life identity.

### IAL 2

**Some confidence in asserted identity**

Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity.

### IAL 3

**High confidence in asserted identity**

Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP

## Authenticator Assurance Levels

### AAL 2

**High confidence in user ownership of credentials**

Provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account.

### AAL 3

**Highest confidence in user ownership of credentials**

Provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account.

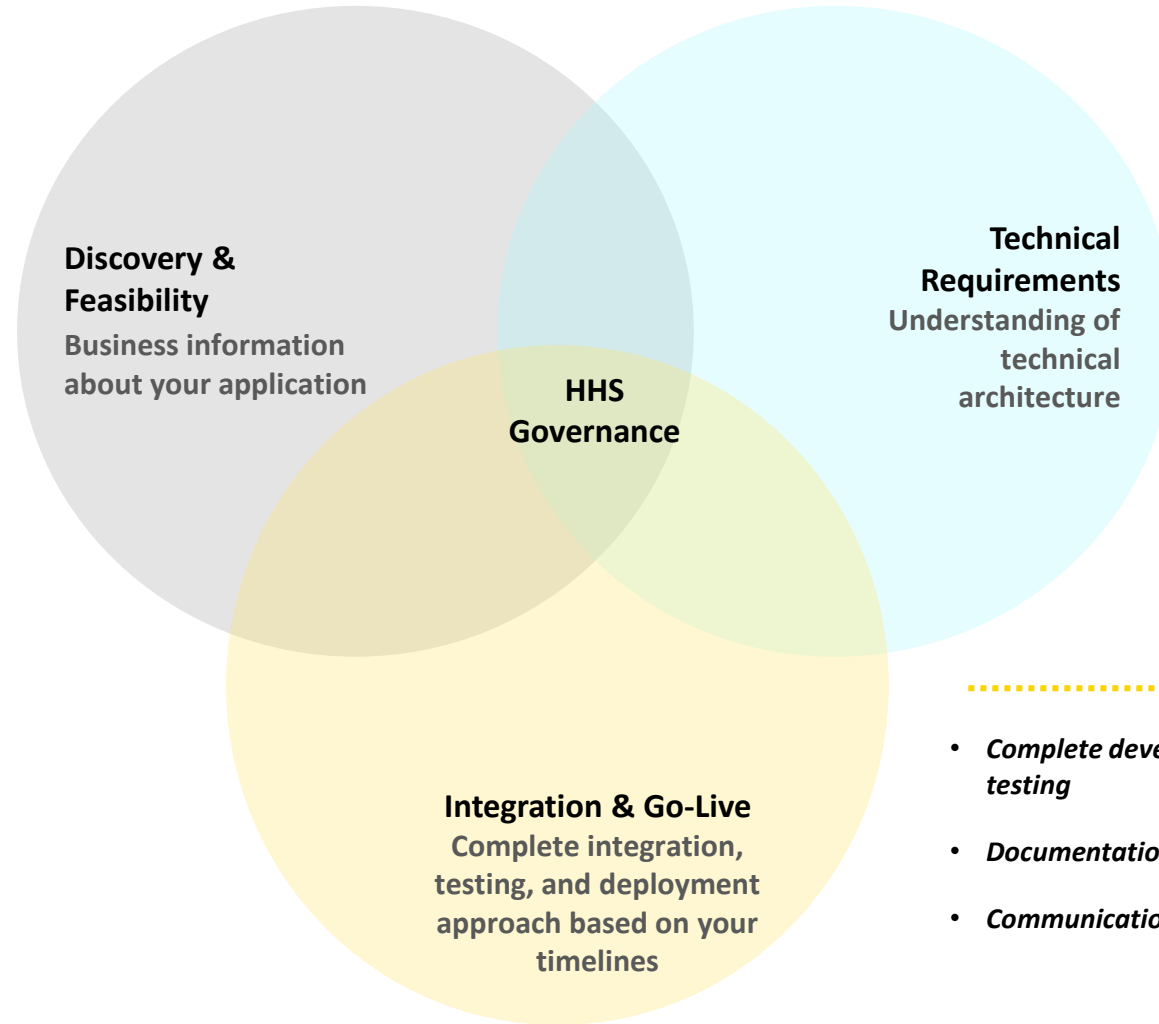


# NextGen XMS – Integration Approach

U.S. Department of Health and Human Services

## HHS Governance considerations include:

Enterprise Performance Lifecycle (EPLC), Interconnect Security Agreement (ISA)/Interagency Agreement (IAA), Security Reviews, Change Management, Customer Impact, and Enterprise Architecture Reviews



- Describe the user population that use your application? E.g.; citizens, state or local government, universities, private institutions
- What is your current registration process and access requirements?
- Do you require users to go through identity proofing?
- What are typical user volumes?

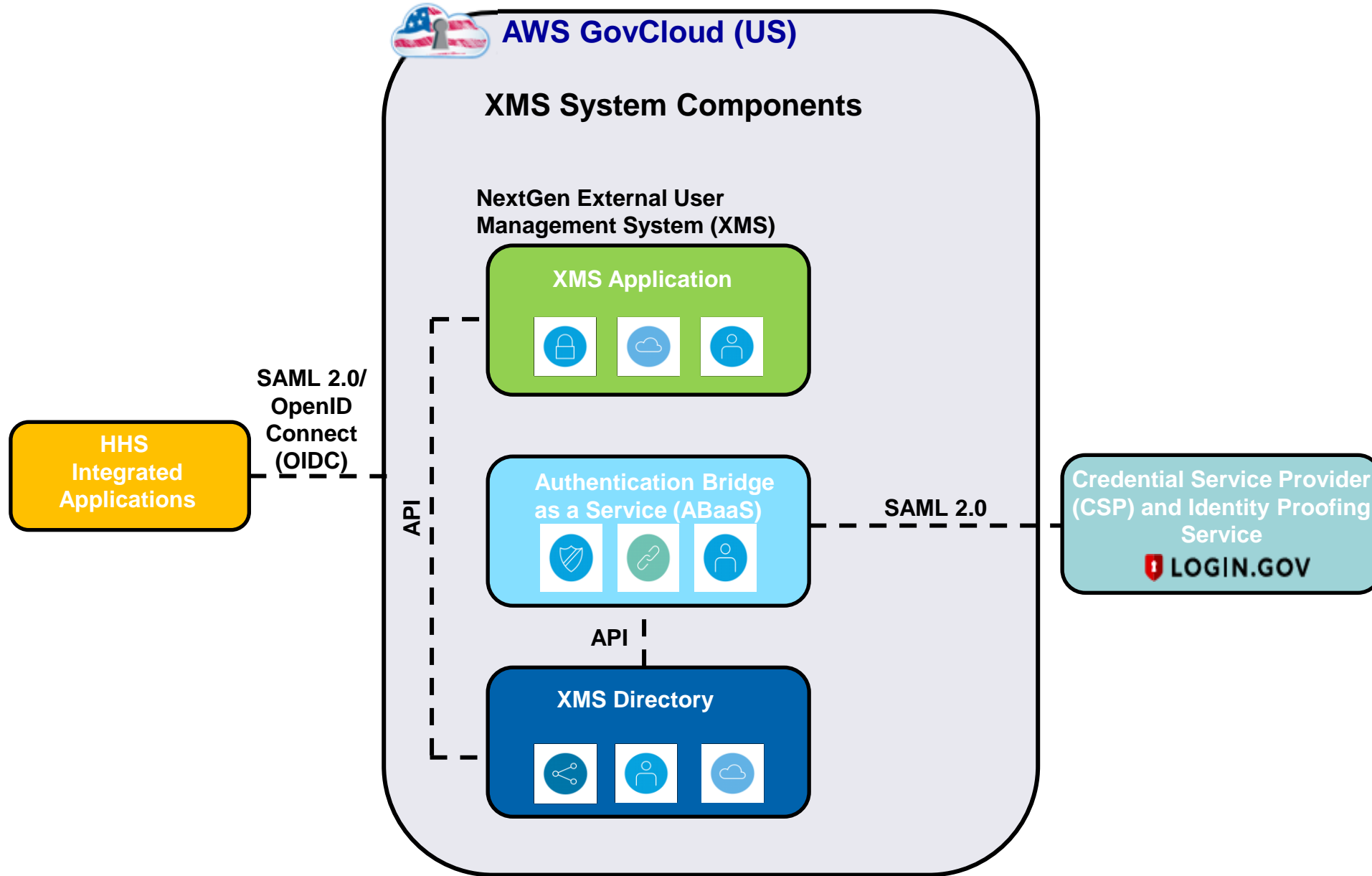
- Does your application support standard protocols like SAML 2.0 or OpenID Connect (OIDC)?
- Is it a SaaS, Cloud Hosted, or on-Prem architecture?

- Complete development and testing
- Documentation, ISA, MOU
- Communication planning



# NextGen XMS – High Level Architecture

U.S. Department of Health and Human Services

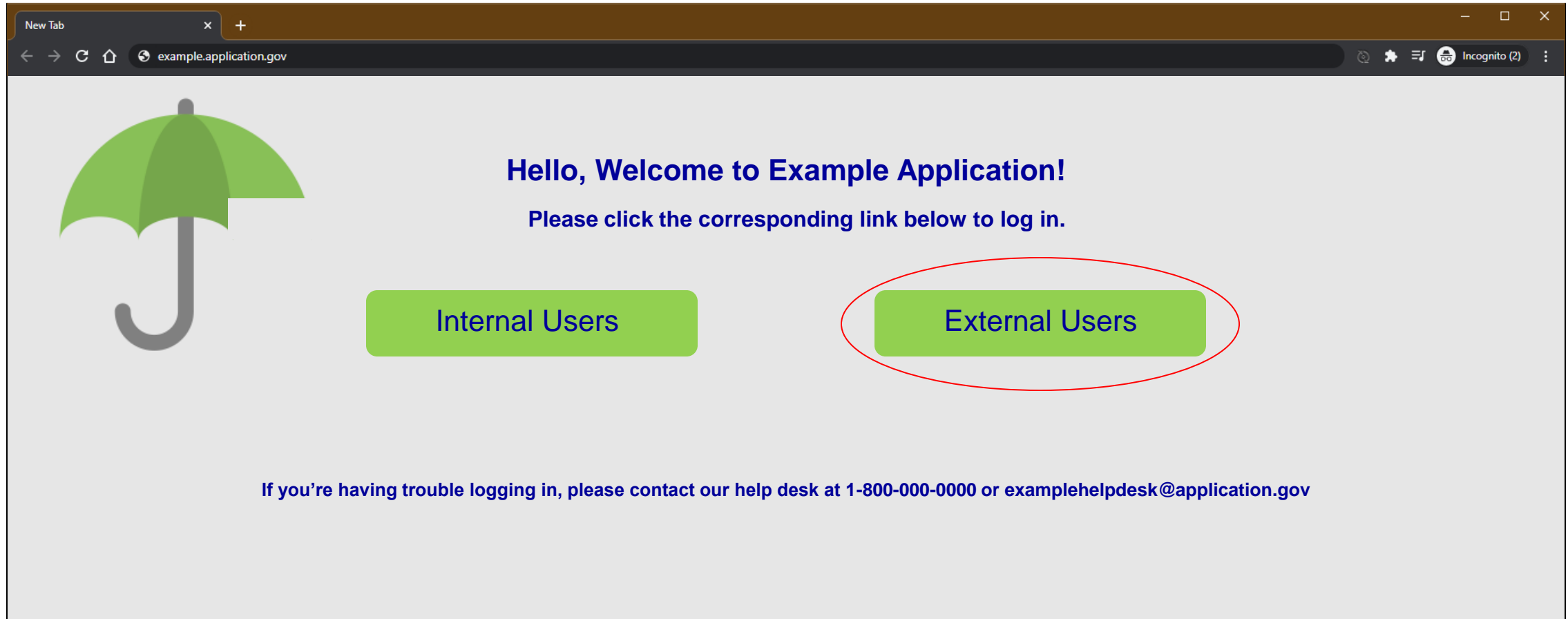




# NextGen XMS Walkthrough – Typical Login Flow

U.S. Department of Health and Human Services

When unauthenticated users arrive at the Target Application’s URL, generally they are presented a “Login Page” showing options to login. For applications that have both internal and external users who authenticate at different levels through different systems, the login page may look something like this:





# NextGen XMS Walkthrough – Typical Login Flow

U.S. Department of Health and Human Services

The 'External Users' button on the previous page will kick off the authentication flow with XMS, and the user will be redirected to the XMS Login Page and asked to authenticate with one of the available options below.

## Login.gov credentials:

The screenshot shows the 'EXTERNAL USER MANAGEMENT SYSTEM' login page. At the top, there are two tabs: 'Login' (highlighted with a blue box) and 'PIV or CAC Login'. Below the tabs, the 'LOGIN.GOV' logo is displayed. The main text reads: 'The External User Management System (XMS) is using a credential provider to allow you to sign in to your account safely and securely. If you do not have an existing Login.gov account, you will be able to create one before you log in.' A blue 'LOGIN' button is highlighted with a red box. At the bottom, there are links for 'Help', 'HHS Privacy Policy', and 'Privacy'.

## PIV/CAC credentials:

The screenshot shows the 'EXTERNAL USER MANAGEMENT SYSTEM' login page with the 'PIV or CAC Login' tab highlighted with a blue box. Below the tabs, the text reads: 'Insert your PIV or CAC into the smart card reader before selecting the "login" option.' A blue 'LOGIN' button is highlighted with a red box. To the right, there is an image of a PIV/CAC smart card. The card displays 'United States Government', 'SEP2018', 'Affiliation: XXX', 'Agency/Department: HEALTH & HUMAN SERVICES (HHS)', 'Expires: 2018SEP30', 'LASTNAME, FIRSTNAME MI.', and 'OpDiv'. A gold chip is visible at the bottom of the card.

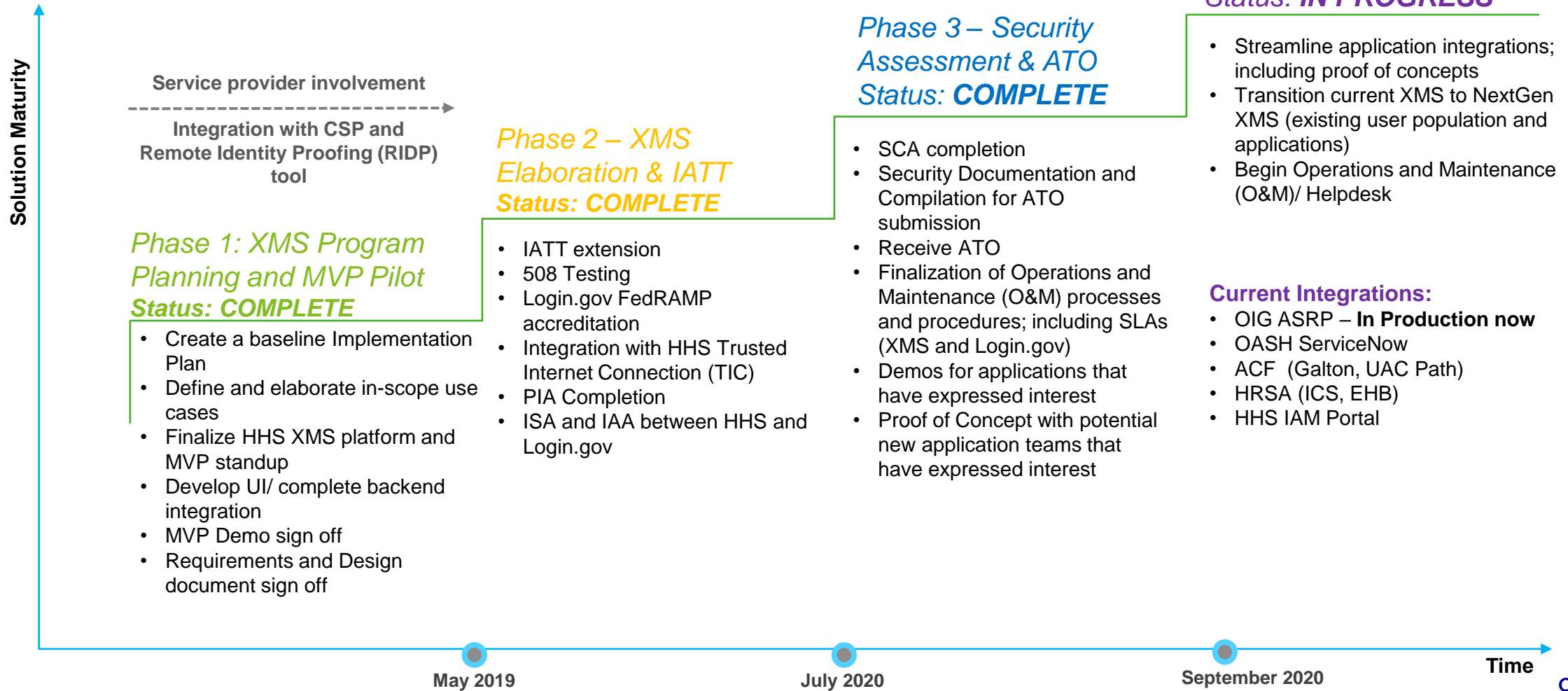




# NextGen XMS Roadmap – Phased Approach

U.S. Department of Health and Human Services

This effort is broken into multiple phases which will continuously deliver incremental business value starting with the Minimally Viable Product (MVP) and leading to production environment with application onboarding:





**Questions?**



U.S. Department of Health and Human Services

---

# NextGen XMS Walkthrough



# NextGen XMS Walkthrough – Login Page

U.S. Department of Health and Human Services

Users have one of two options for authenticating into XMS:

Login.gov credentials:

HHS.gov | EXTERNAL USER MANAGEMENT SYSTEM U.S. Department of Health and Human Services

Select a Login Method

Login | PIV or CAC Login

**LOGIN.GOV**

The External User Management System (XMS) is using a credential provider to allow you to sign in to your account safely and securely.

If you do not have an existing Login.gov account, you will be able to create one before you log in.

**LOGIN**

[? Help](#) [i HHS Privacy Policy](#) [i Priva](#)

PIV/CAC credentials:

Login | **PIV or CAC Login**

Insert your PIV or CAC into the smart card reader before selecting the "login" option.

**LOGIN**


United States Government

**SEP2018**

AMERICAN  
XXX  
Agency/Department  
HEALTH & HUMAN  
SERVICES (HHS)  
Expires  
2018SEP30

LASTNAME,  
FIRSTNAME MI.

**OpDiv**





# NextGen XMS Walkthrough – Logging In via Login.gov or PIV/CAC

U.S. Department of Health and Human Services

**Users will be redirected to Login.gov’s landing page to enter their credentials and second factor of authentication:**

**Users will be directed to register their PIV/CAC upon first-time log in to show ownership of account:**



# NextGen XMS Walkthrough – User Dashboard

U.S. Department of Health and Human Services

Upon successful authentication, users will be taken to their dashboard:

HHS.gov

EXTERNAL USER MANAGEMENT SYSTEM

[My Profile](#) | [Logout](#)

Home

App Management

Request Status

## WELCOME, TESTERONE@TEST.COM!

Select from the icons below to access your applications.

### My Applications

### Notifications

No recent notifications

[? Help](#) [i HHS Privacy Policy](#) [i Privacy Act Statement](#)



# NextGen XMS Walkthrough – My Profile

U.S. Department of Health and Human Services

From the My Profile page, users will have the option to update their profile, or request affiliation with an organization:

- Home
- App Management
- Request Status

## MY PROFILE

### Profile Details

First Name	Password <b>LOGIN.GOV</b>
Middle Name	Notifications Email <b>testerone@test.com</b>
Last Name	

[EDIT NOTIFICATIONS EMAIL](#)

### PIV or CAC Details

No PIV or CAC information

### Organization Affiliation Details

No organization affiliation

[EDIT AFFILIATION](#)

### Link a PIV or CAC

Insert your PIV or CAC into the smart card reader before selecting the link option.

[LINK CARD](#)

## MY PROFILE

### Profile Details

First Name	Password <b>LOGIN.GOV</b>
<b>Tester</b>	Notifications Email <b>testerone@test.com</b>
Middle Name	
Last Name	Identity Verified <b>Verified</b>
<b>One</b>	

[EDIT NOTIFICATIONS EMAIL](#)

### PIV or CAC Details

Email  
**testerone@test.com**

EDIPI/FASC-N  
**<EDIPI/FASC-N>**

UPN  
**<UPN>**

Subject DN  
**<Subject DN>**

Expiration Date  
**<Expiration Date>**

Issuer  
**<Issuer>**

[EDIT EMAIL](#)

### Organization Affiliation Details

Organization	Role
The Targaryens	Admin

[EDIT AFFILIATION](#)

### Link a PIV or CAC

Insert your PIV or CAC into the smart card reader before selecting the link option.

[REPLACE CARD](#)



# NextGen XMS Walkthrough – Affiliation Requests

U.S. Department of Health and Human Services

From the Organization Affiliation page, you may request to affiliate as a member or an administrator for an organization:

### Manage Your Organization Affiliation

**Affiliation Form**

Please complete all fields to affiliate with an organization:

Select an Organization

Select a Role  
Member

**SUBMIT** **CANCEL**

**i** **Don't see your organization listed?**  
Click here to learn how you can register your organization with XMS



### Manage Your Organization Affiliation

**User Information**

Please complete the fields below to affiliate with an organization:

First Name

Middle Name (optional)

Last Name

**CONTINUE** **CANCEL**



### Manage Your Organization Affiliation

**Submission Confirmation**

**✓** **Affiliation Request Submitted**  
Your affiliation request has been sent to your Organization Administrator for review and approval. If you have any questions regarding your request, please contact your Organization Administrator.

[Return to Dashboard](#)





# NextGen XMS Walkthrough – Organization Registration Request

U.S. Department of Health and Human Services

**Users requesting to register an organization must perform identity proofing, understanding rules for submitting request:**

## Identity Proofing

As part of the Organization or Organization Administrator registration process, you are required to undergo identity proofing. For users that do not have a PIV or CAC, please follow the instructions on the following screens. **For users with a valid and active PIV or CAC, insert your card into a smart card reader before selecting the "Continue" button.**

Select a method of identity proofing from the options below:

- I have a PIV or CAC
- I do NOT have a PIV or CAC

CONTINUE

CANCEL

### Registration Information

#### Organization Administrator FAQ

If your organization has not been registered with the External Management System (XMS), you or another employee of your organization will need to complete the registration process before being able to access organizational features. General information regarding the organization registration process is outlined below:

#### Who can complete the organization registration process?

Anyone who is an employee of the organization being requested and has a valid PIV or CAC is able to complete the process. The user completing the registration process will also be required to become the Organization Administrator, which involves successfully completing an identity proofing process (more information can be found by clicking the [Organization Administrator FAQ](#) link on this page).

#### What information is needed to complete the process?

A Federal Sponsor's first name, last name, and email address are required. If you do not have access to this information, you can either gather the required information from someone within your organization, or inform another employee who does know the information to complete the organization registration process from their XMS account.

CONTINUE

CANCEL

## Terms and Conditions

Please read the following terms and conditions carefully before continuing with the registration process.

All individuals that are creating an organization (or entity) within the NextGen External User Management System (XMS) must comply with the following terms and conditions:

#### Ownership

XMS is the property of the U.S. Department of Health and Human Services (HHS), and is for authorized users only. The system is for official federal government business only. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative penalties.

#### Responsibilities

As the person creating or registering the organization with XMS, you are responsible for maintaining the integrity of, and are held accountable for, everything done within and on behalf of this organization.

#### Organization Registration

By registering this organization in XMS, you are attesting that the organization being created is a legal and real entity, subject to all federal and state laws. Information entered into XMS shall

I acknowledge and understand my responsibilities and agree to comply with the Terms and Conditions Agreement for XMS

CONTINUE

CANCEL

## Complete Registration Request

### Registration Form

Please complete the following form to continue the registration process:

Organization Name

Organization Classification

Federal Sponsor Name

Federal Sponsor Email

Business Justification (max. 2,000 characters)

SUBMIT

CANCEL



# NextGen XMS Walkthrough – Application Access Request

U.S. Department of Health and Human Services

From the **Application Management** tab, you may request access to an application:

The screenshot shows the 'Application Management' section of the NextGen XMS interface. At the top, there are navigation tabs: 'Home', 'App Management' (which is active), and 'Request Status'. Below the tabs, the main heading is 'APPLICATION MANAGEMENT'. Underneath, there is a sub-heading 'Request Application Access' and a text prompt: 'Request applications to be added to your dashboard using the form below.' followed by an information icon. The form contains a dropdown menu with the text 'Please select an application from the list below:' and a blue 'SUBMIT' button. To the right of the form is a dark blue box with the text 'My Applications'.

## Sample configurations:

This notification card has a green vertical bar on the left and a checkmark icon. The text reads: **Request Completed**  
Access has been granted. Return to the XMS Dashboard to confirm access.  
At the bottom, there is a blue link: [Return to XMS Dashboard](#). A close button (X) is in the top right corner.

This notification card has a green vertical bar on the left and a checkmark icon. The text reads: **Request Submitted**  
Your request has been successfully submitted. Click the link below to return to the XMS dashboard, or close this window to continue requesting access.  
At the bottom, there is a blue link: [Return to XMS Dashboard](#). A close button (X) is in the top right corner.

This notification card has an orange vertical bar on the left and an exclamation mark icon. The text reads: **XMS-6002: Application Access Request Not Submitted**  
This application requires you to be affiliated with its organization in order to access it. Please affiliate first and then submit the application request.  
At the bottom, there is a blue link: [Return to XMS Dashboard](#). A close button (X) is in the top right corner.



# NextGen XMS Walkthrough – Approvals

U.S. Department of Health and Human Services

From the Pending Items tab, users can review and act upon requests submitted to them:

Home App Management User Management **Pending Items (3)** Request Status

## PENDING ITEMS

Review and manage user requests. For more information regarding the approval and/or rejection of requests, please refer to the guidelines in our help pages.

User Requests			
Requester	Request Type	Request Date	Action
System Admin	Application Access	03/20/2020	<a href="#">REVIEW</a>
System Admin	Member Affiliation	03/20/2020	<a href="#">REVIEW</a>
System Admin	Organization Registration	03/20/2020	<a href="#">REVIEW</a>

## Sample Approval Requests:

### Details

<b>First Name</b> System	<b>Request Date</b> 03/20/2020
<b>Last Name</b> Admin	<b>Request Type</b> Organization Registration
<b>Email</b> ngxms06@mailinator.com	<b>Organization</b> Pharma Inc
<b>Business Justification</b> To create the pharma, inc organization.	

### Details

<b>First Name</b> System	<b>Request Date</b> 03/20/2020
<b>Last Name</b> Admin	<b>Request Type</b> Application Access
<b>Email</b> ngxms06@mailinator.com	<b>Application</b> Google

### Details

<b>First Name</b> System	<b>Request Date</b> 03/20/2020
<b>Last Name</b> Admin	<b>Request Type</b> Member Affiliation
<b>Email</b> ngxms06@mailinator.com	<b>Organization</b> The Targaryens

This request requires confirmation of the following:

- I have verified that the first name and last name provided by the user during the affiliation request process match the user's true identity
- I have verified the requester is a member of my organization
- I hereby affirm that I have vetted the user to the best of my ability and accept responsibility for the validation of the user's identity

✓ APPROVE

✗ REJECT

BACK

✓ APPROVE

✗ REJECT

BACK

✓ CONFIRM

✗ DENY

BACK



# NextGen XMS Walkthrough – User Management

U.S. Department of Health and Human Services

From the User Management tab, Org Admins can manage users within their organization:

Home App Management **User Management** Pending Items (1) Request Status

## USER MANAGEMENT

View and manage user accounts that have been affiliated with your organization. ⓘ

### Search Users

First Name Middle Name Last Name

Email XID Role

**SEARCH** **RESET**

### Organization Users

Name	Email Address	Role	XID	Actions
a.jury@mailinator.com	a.jury@mailinator.com	Admin	100000348	<b>VIEW</b> <b>REMOVE</b>
Alexa L. Jury	a.ljury@mailinator.com	Admin	100000400	<b>VIEW</b> <b>REMOVE</b>

### USER DETAILS:

**First Name:** a.jury@mailinator.com  
**Middle Name:** undefined  
**Last Name:** undefined  
**Email:** a.jury@mailinator.com  
**Role:** Admin  
**XID:** 100000348  
**Organization:** The Targaryens

### USER REMOVAL:

**First Name:** John  
**Middle Name:** T.  
**Last Name:** Smith  
**Email:** john.t.smith@hhs.gov  
**Role:** Member  
**XID:** 100000029  
**Organization:** Organization 1  
**Comments:**

**REMOVE** **BACK**



# NextGen XMS Walkthrough – Application Management

U.S. Department of Health and Human Services

From the Application Management tab, App Admins can manage access for their applications:

Home **App Management** User Management Pending Items (1) Request Status

### APPLICATION MANAGEMENT

Request applications to be added to your dashboard using the form below. ⓘ

#### Request Application Access

Please select an application from the list below:

#### My Applications

- Bing
- Google

### ACCESS MANAGEMENT

View and manage user accounts that have been granted access to your application. ⓘ

#### Search Users

First Name  Middle Name  Last Name

Email  XID  Application

#### Application Users

Name	Email Address	Application	XID	Actions
Jane Smith	janesmith.xms@mailinator.com	Google	100000259	<input type="button" value="VIEW"/> <input type="button" value="REMOVE"/>
Kenneth M. Trumpoldt	xmstestlgauth3@mailinator.com	Google	100000353	<input type="button" value="VIEW"/> <input type="button" value="REMOVE"/>

### USER DETAILS:

---

**First Name:** Jane  
**Middle Name:** undefined  
**Last Name:** Smith  
**Email:** janesmith.xms@mailinator.com  
**XID:** 100000259  
**Application:** Google

### ACCESS REMOVAL:

---

**First Name:** John  
**Middle Name:** T.  
**Last Name:** Smith  
**Email:** john.t.smith@hhs.gov  
**XID:** 100000012  
**Application:** Application 1  
**Comments:**



# NextGen XMS Walkthrough – Request Status

U.S. Department of Health and Human Services

From the Request Status tab, all users can view and manage their submitted requests:

Home App Management User Management Pending Items (1) Request Status

## REQUEST STATUS

View and manage your submitted requests. i

### Search Requests

Status:  Request Type:  Keyword i

### My Requests

Keyword	Request Type	Date Submitted	Status	Actions
Organization 3	Organization Registration	09/22/2020	PENDING	<input type="button" value="VIEW"/> <input type="button" value="CANCEL"/>
Application 1	Application Access	09/14/2020	EXPIRED	<input type="button" value="VIEW"/>
Organization 2	Admin Affiliation	09/02/2020	APPROVED	<input type="button" value="VIEW"/>
Organization 1	Member Affiliation	07/24/2020	DENIED	<input type="button" value="VIEW"/>

Scroll to view more columns in the table

### REQUEST DETAILS:

**Application:** Application 1

**Request Type:** Application Access

**Date:** 09/14/2020

**Status:** EXPIRED

### REQUEST CANCELLATION:

**Organization:** Organization 5

**Request Type:** Organization Registration

**Date:** 09/22/2020

**Status:** PENDING

**Federal Sponsor Name:** XMS Test

**Federal Sponsor Email:** xms.test@hhs.gov

**Business Justification:**  
Creating an organization in XMS