



# RSA: From History to Hands-On

**Khaled Abouelnaga** | Senior Manager Technical Support

**Amr Esawy** | Principal Technical Support Engineer


**Ahmed Hamza** | Senior Technical Support Engineer

**Ahmed Galal** | Technical Support Engineer

# Agenda

- Brief History about RSA
- Multifactor Authentication (MFA) Fundamentals
- RSA Overview & Products
- Career Opportunities: What's in it for You?
- Project Overview: Milestones & Flow
- Technical Project Deep Dive: Scenario & Architecture
  - Identity Router (IDR)
  - Identity Source (IS)
  - My Page
  - RSA MFA Agent for Microsoft Windows
  - RADIUS
  - Security Assertion Markup Language (SAML)





**Every digital handshake, every secure online transaction, every protected piece of data - RSA has been a silent guardian.**





# Brief History about RSA



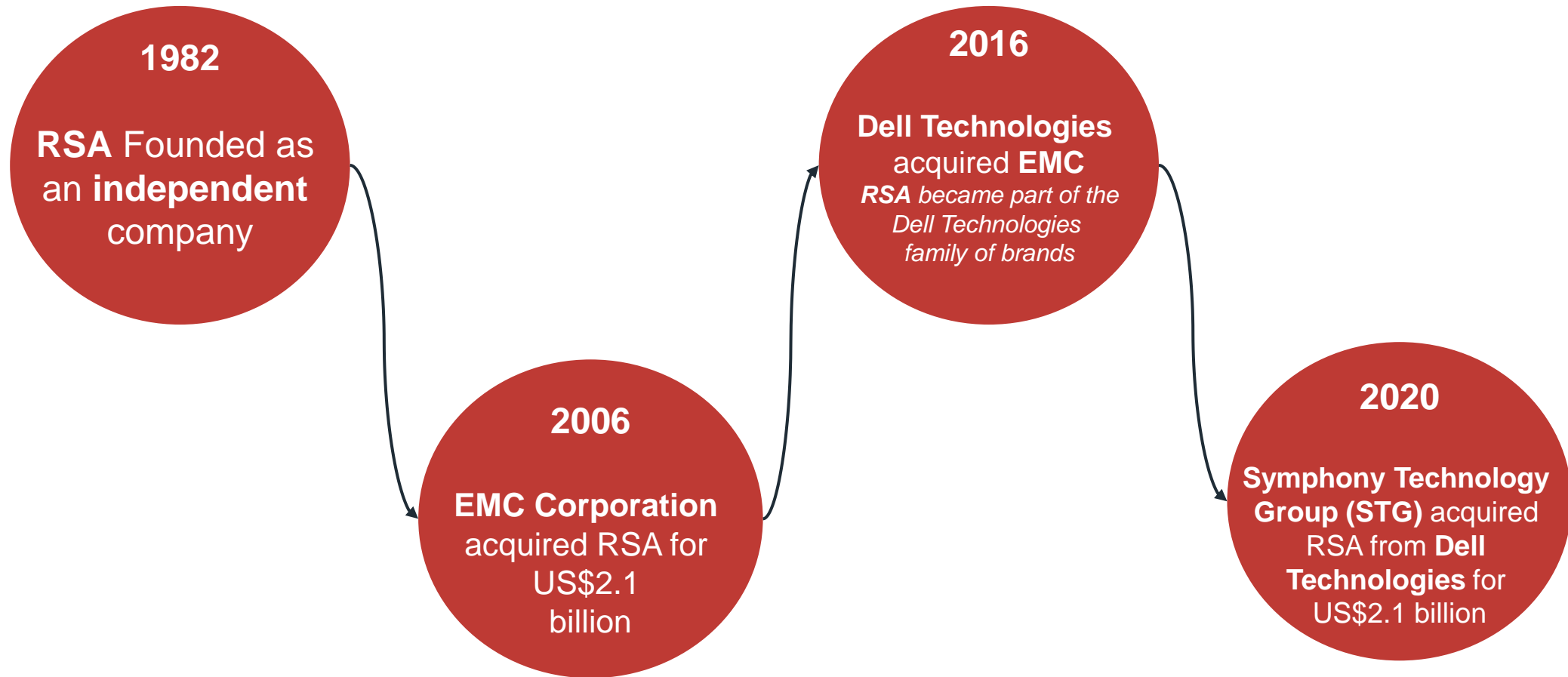
# Brief History about RSA

- **RSA**, an **American computer and network security company** founded in **1982** by **Ron Rivest**, **Adi Shamir**, and **Leonard Adleman**, named after their initials emerged from their pioneering work on **asymmetric cryptography**.
- It is headquartered in **Burlington, Massachusetts**. It maintains a global presence with regional and international offices across the **Americas, Europe, Asia, Africa, and Australia**.



# Brief History about RSA

## ■ RSA's Acquisition History







# Multifactor Authentication (MFA) Fundamentals



# Multifactor Authentication (MFA) Fundamentals

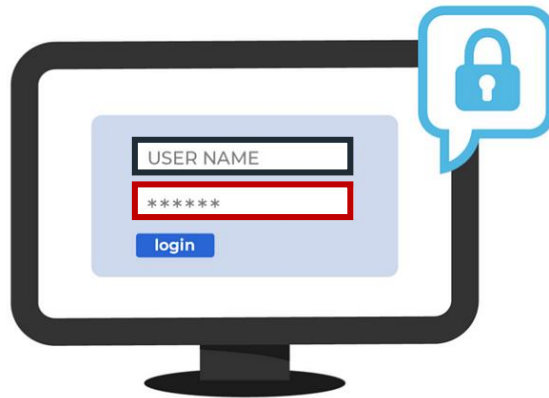
IAAA

Identification



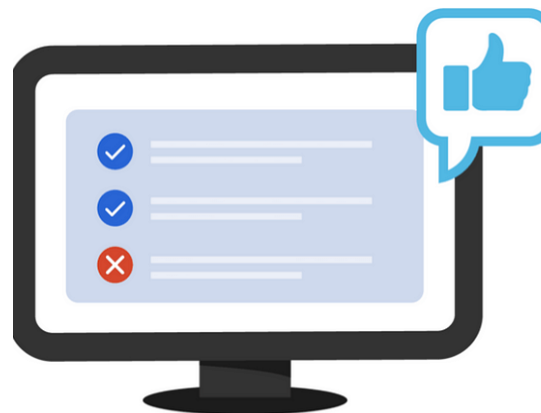
Process where the user claim's identity to a system

Authentication



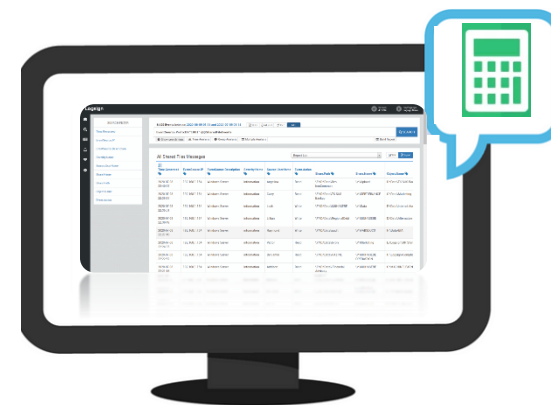
Verifying identity of user to a system

Authorization



Giving users permission to access a resource

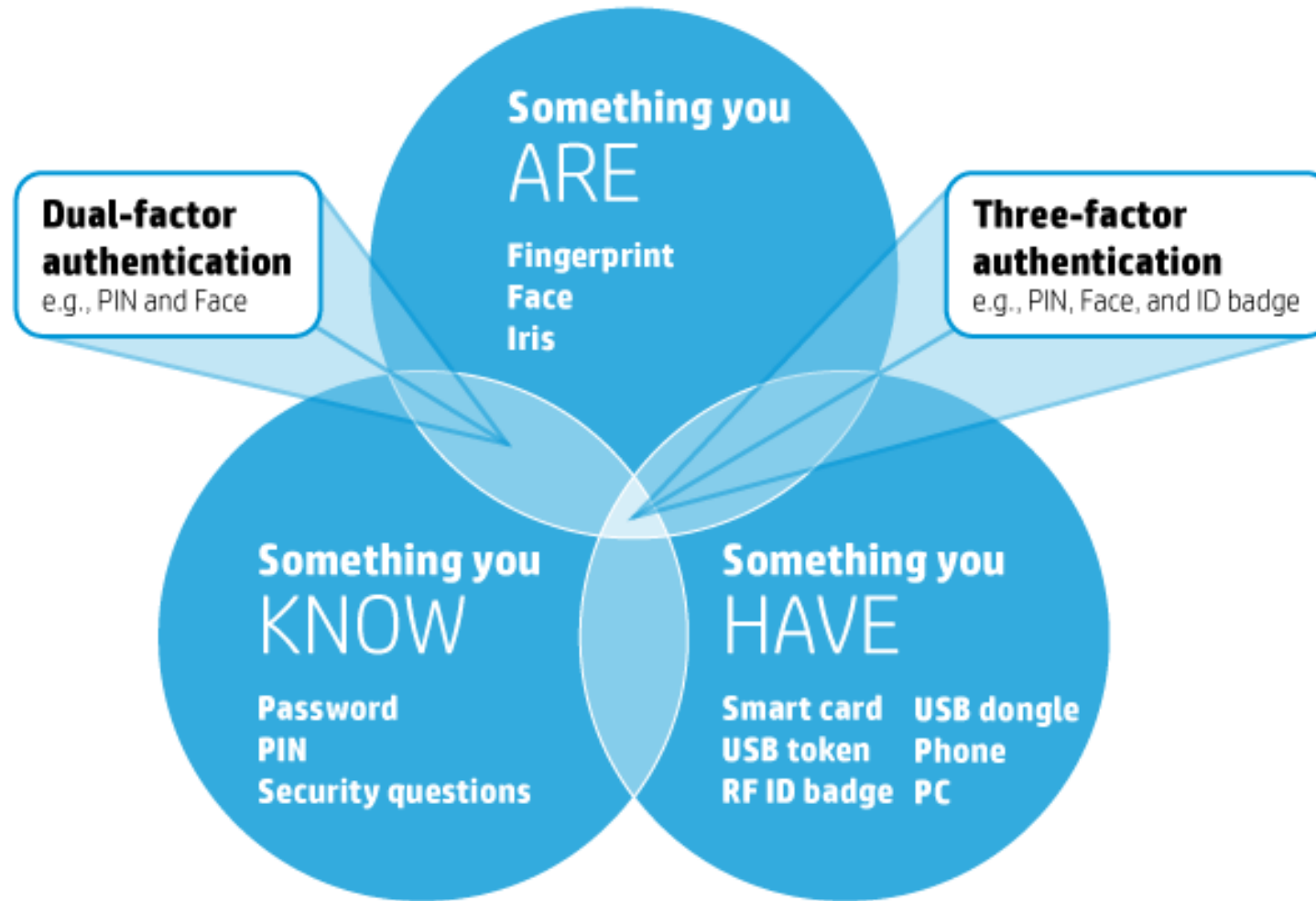
Accounting



What resources and pages are being accessed?  
[Logging]



# Multifactor Authentication (MFA) Fundamentals





# RSA Overview & Products





# RSA Overview & Products

- Industries We Secure



**Government**



**Energy**



**Financial**



**Healthcare**

# RSA Overview & Products

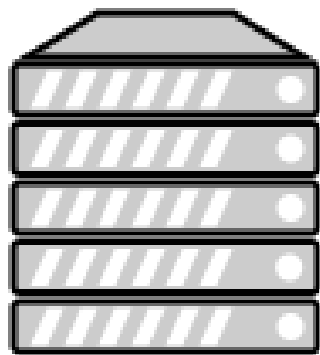
**RSA** focus on delivering the **AAA** framework. This is represented into **two products**





# RSA Products

- **RSA - SecurID** provides On-premise solution (Authentication Manager – AM) and Cloud solution (Cloud Authentication Service - CAS) that could be used separately or combined into one multifactor (MFA) Hybrid solution.



**RSA**

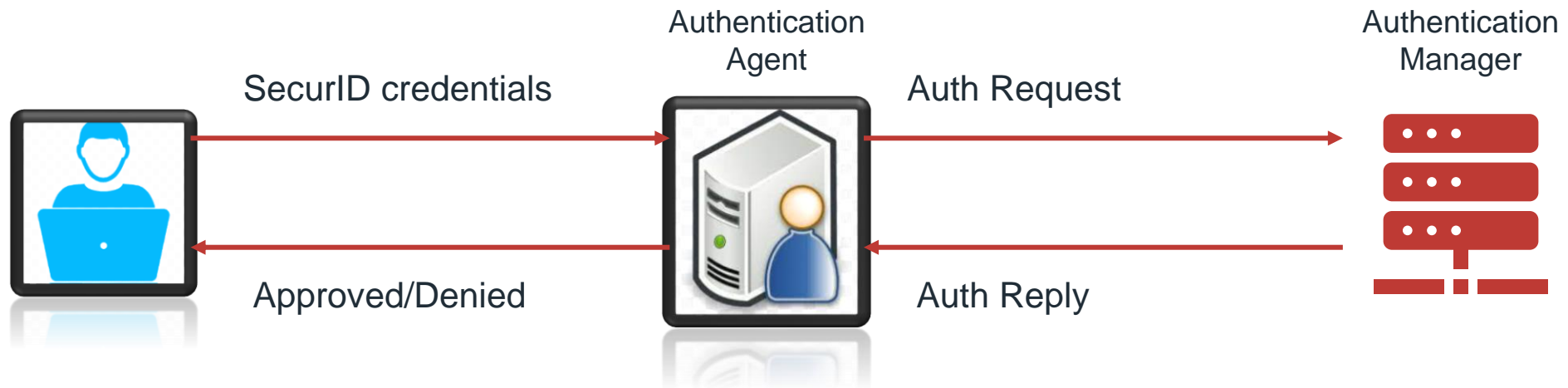
**On-Premise Solution**  
RSA Authentication Manager



**Cloud Solution [ID PLUS]**  
RSA Cloud Authentication Service

# RSA Products: Authentication Agents

- Authentication Agent acts as a **gatekeeper**, challenges users for their **RSA credentials** then **passes them to Auth Manager**.
- Agents could be a **3<sup>rd</sup> party device**: Firewall, VPN gateway, router, switch..etc.  
Or could be a software application provided by RSA to protect Windows/Linux machines...etc.





# RSA Products: Authenticators

- RSA authenticators, also known as **tokens**, generate **one-time authentication credentials** for a user.
- Users should have **hardware** or **software token** to be able to authentication with AM or CAS.

*Hardware SID700*



*Hardware SID800*



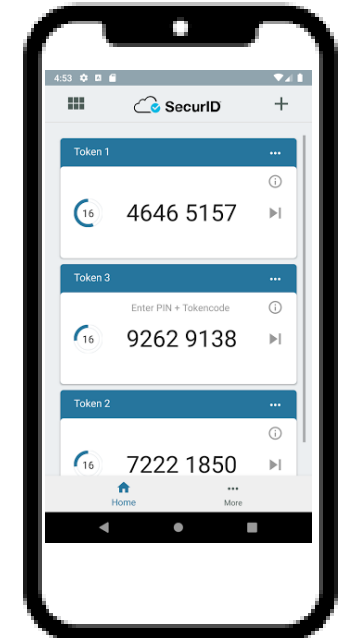
*DS100*



*iShield*



*RSA Authenticator App for Windows, iOS and Android phones*





# Career Opportunities: What's in it for You?



Securing the  
**most secure.**

# What is in it for you?

01

## Perfect simulation

Fully responsible for implementing and troubleshooting their environment, simulating real-world corporate scenarios

02

## Practical Experience

Students gain real-world experience with industry-standard technologies, enhancing their skills and employability.

03

## Career Opportunities

Improved job prospects as students become proficient in RSA tools, making them attractive to potential employers and increasing their chances of being shortlisted for RSA vacancies.





# Project Overview: Milestones & Flow



# Background

1

## Identity

- Install AD and IDR.
- Create Identity Source
- Create Access Policy.
- Protect MyPage with Authenticate OTP.
- MyPage Customization.

2

## Protect Access

- Install Windows machine and MFA agent.
- Apply GPOs to challenge a certain group.
- Install ntrading (RADIUS Client)
- Challenge users with Approve and device biometrics

3

## Protect Access

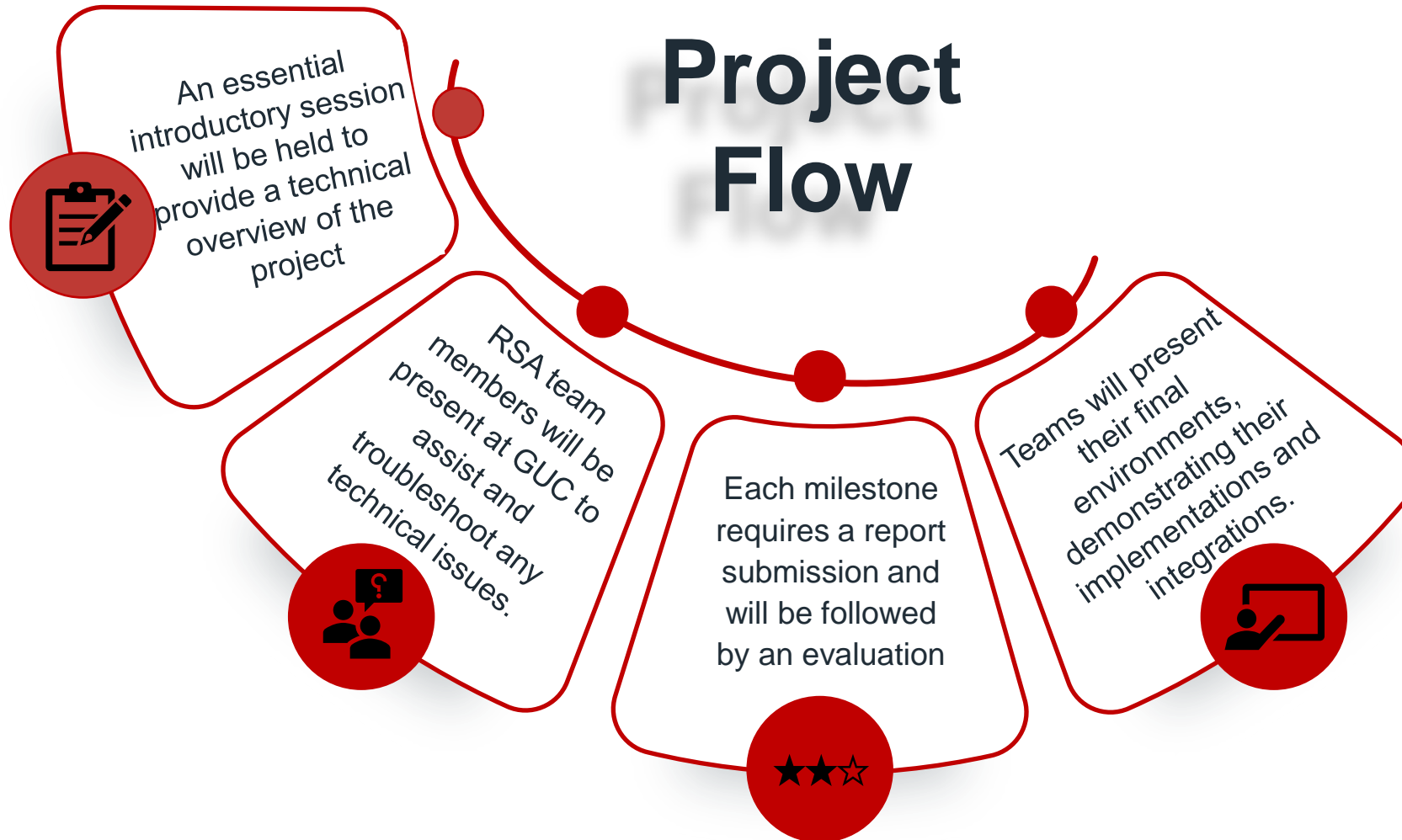
- Integrate the CAS with SAML apps such as Salesforce and [sptest.iamshowcase.com](https://sptest.iamshowcase.com)

4

## Stress Testing

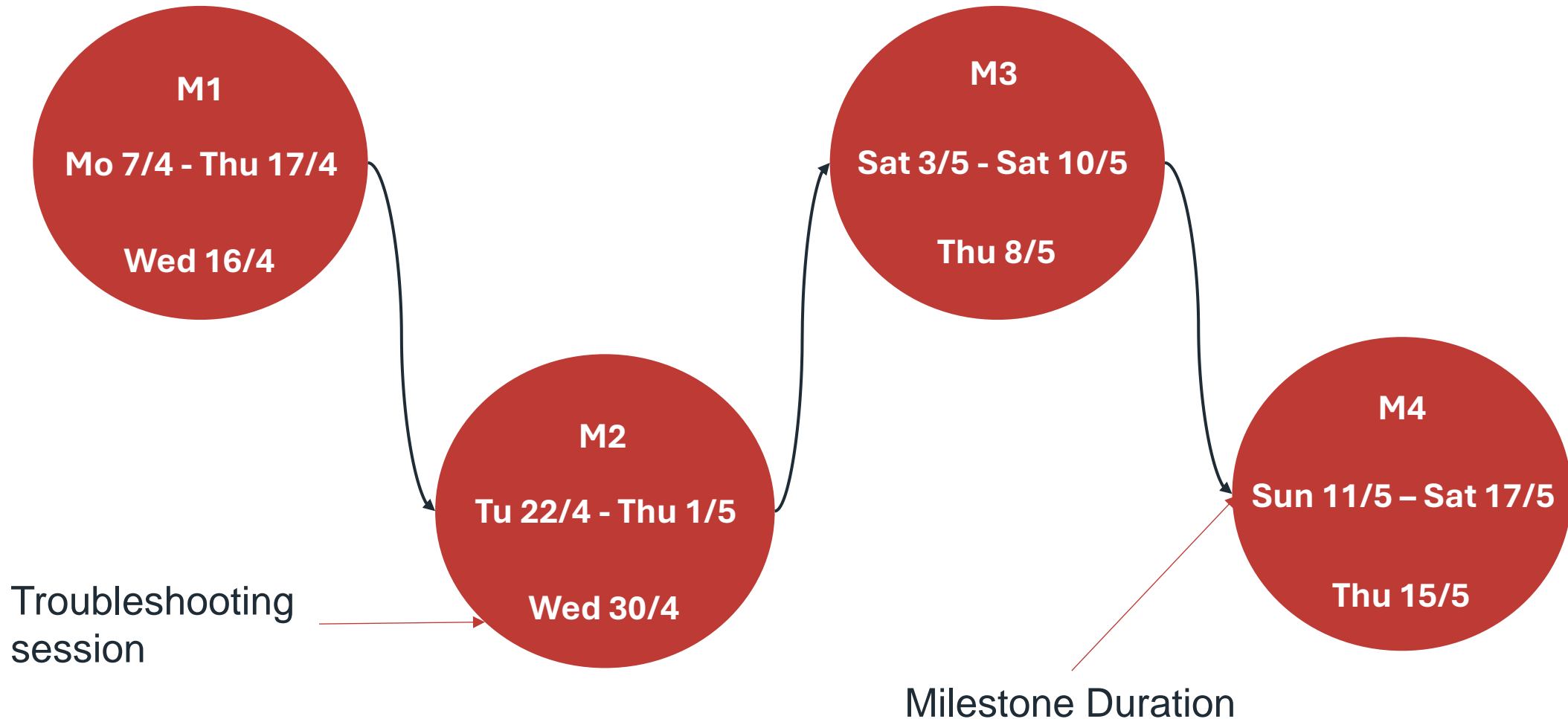
- Students will use JMeter to do a performance test to see how the Cloud console handles REST API calls and how the IDR manages RADIUS requests, providing a comprehensive performance dashboard for multiple use cases

# Project Flow





# Milestones and troubleshooting sessions Timeline





# Technical Project Deep Dive: Scenario & Architecture





# Identity Router

Explanation





# Identity Router

IDR is software that enforces authentication and access for protected resources.

- **Communication:**

- Connects with Cloud Authentication Service, Identity Sources, and Authentication Manager.

- **Key Benefits:**

- Enterprise Connector: Bridges LDAP and Authentication Manager to the cloud.
- RADIUS Support: Built-in RADIUS server for authentication.
- Single Sign-On (SSO): Enables SSO via the IDR portal.

- **Interfaces:**

- Single Interface: Used for both management and portal
- Dual Interface: Separate interfaces for management and portal

- **Deployment Options:**

- Can be deployed on VM, Hyper-V, AWS, or Auth Manager 8.5+ (Embedded IDR).

# Identity Router

Enable SecurID Token Users to Access Resources Protected by the Cloud Authentication Service

User opens application portal and provides primary and/or additional credentials if required by access policy.

- 1 Identity router sends user credentials to identity source for verification.

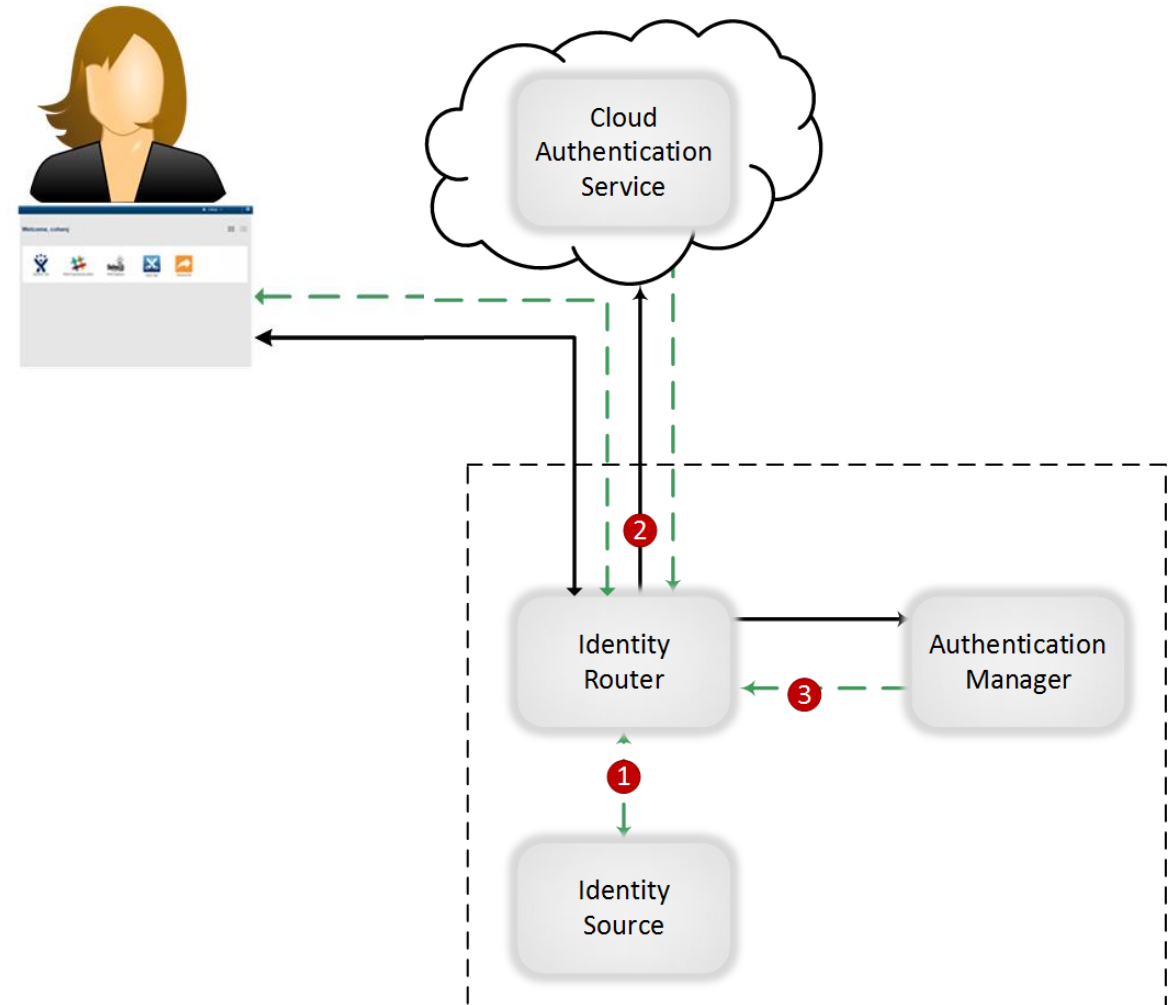
User is now signed in to the portal. User clicks an app icon to open an app.

- 2 Identity router asks the Cloud Authentication Service to check access policy for this app. In this case, a SecurID Token is required.

User provides SecurID Tokencode based on policy requirement.

- 3 Identity router sends SecurID Tokencode to Authentication Manager for validation. Authentication Manager returns approval.

User is granted access to the app.



# Identity Sources

An identity source is a repository in the Cloud Authentication Service (CAS) that represents one primary LDAP directory server, its replicas, and/or a Unified Directory. Cloud Authentication Service includes the following types of identity sources:

- Azure Active Directory (SCIM)
- Microsoft Active Directory
- Local
- SCIM Managed
- RSA Authentication Manager Internal Database



# Assurance Level

- Assurance levels define the authentication methods required to access applications or authentication clients (relying party or RADIUS client) during authentication. RSA provides three assurance levels: High, Medium, and Low. Each level indicates the relative strength and security of the authentication methods within that level

## Assurance Levels



Cancel

Save

You are permitted to use only the authenticators you have purchased.

An assurance level defines which authentication methods can be used for additional authentication. To access the application, users must successfully authenticate using one option from an assurance level. The first option configured in the list for each level is the default presented to the user for the first authentication. Users can select another method if others are available.

High Assurance Level	Medium Assurance Level	Low Assurance Level
<div>SecurID OTP and Approve</div>	<div>Device Biometrics</div>	<div>Approve</div>
<div>FIDO and Approve</div>	<div>OATH HOTP</div>	<div>Authenticate OTP</div>
<div>+ ADD</div>	<div>+ ADD</div>	<div>SecurID OTP</div>
		<div>+ ADD</div>

# Access Policies

- Access policies determine which users can complete authenticator registration and access applications or authentication clients. Policies also determine whether those users must perform additional authentication, after primary authentication, in order to use the resources.

RSA evaluates an access policy by performing the following high-level steps.

1. RSA identifies the target user population for the policy using the **Identity Source** field on the Identity Source
2. RSA goes to the first rule set and uses the **Target Population** field to determine if the rule set applies to all users or only to users who match LDAP user attribute criteria.
3. RSA uses the **Access** field to determine if user access is allowed or denied or determined based on contextual conditions.
4. RSA uses the **Additional Authentication** field to determine if additional (step-up) authentication is required.
5. If multiple rule sets are used, RSA continues to process each one in sequence.



# My Page

Cloud-hosted SSO that empowers users to do more





# My Page

- My Page enhances Single Sign-On (SSO) by providing a centralized portal for quick access to multiple applications. It offers self-service functionality, credential management, and a customized user experience. As a cloud-hosted SSO solution, it simplifies access for users while reducing IT workload by enabling self-service device registration and management.
- **Features & Benefits of My Page (SSO Solution)**
  - Unified Portal: Centralized access for SSO and credential management.
  - Self-Service Registration: Enables users to register any cloud authenticator.
  - Reduced Helpdesk Load: Minimizes IT support requests through self-service.
  - Cloud-Hosted: Enhances efficiency and reduces costs.
  - QR Code Enrollment: Simplifies the setup process.
  - Secure Access: Supports modern authentication methods.
  - Custom Branding: Allows organizations to personalize branding and domains.

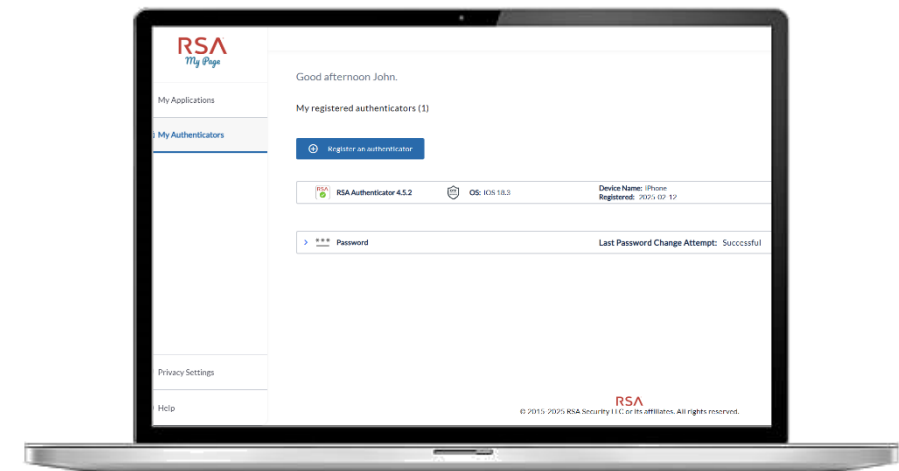
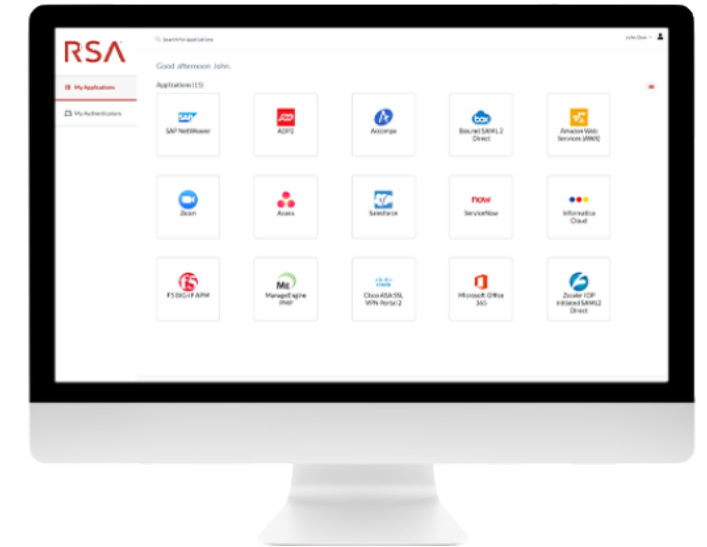
# My Page

## ■ My Applications

- The My Applications view enables users to securely and conveniently leverage SSO to access their applications.

## ■ My Authenticators

- In the My Authenticators view, users can register and manage authenticators, using intuitive QR codes for self-enrollment.





# RSA MFA Agent for Microsoft Windows

Explanation and Implementation



Securing the  
**most secure.**

# Agent-Server Communication

When users try to sign into or unlock their Windows computers, the MFA Agent communicates with either Cloud Authentication Service or Authentication Manager to manage authentication.

- **Protocol:**

- AM => REST
- CAS => REST

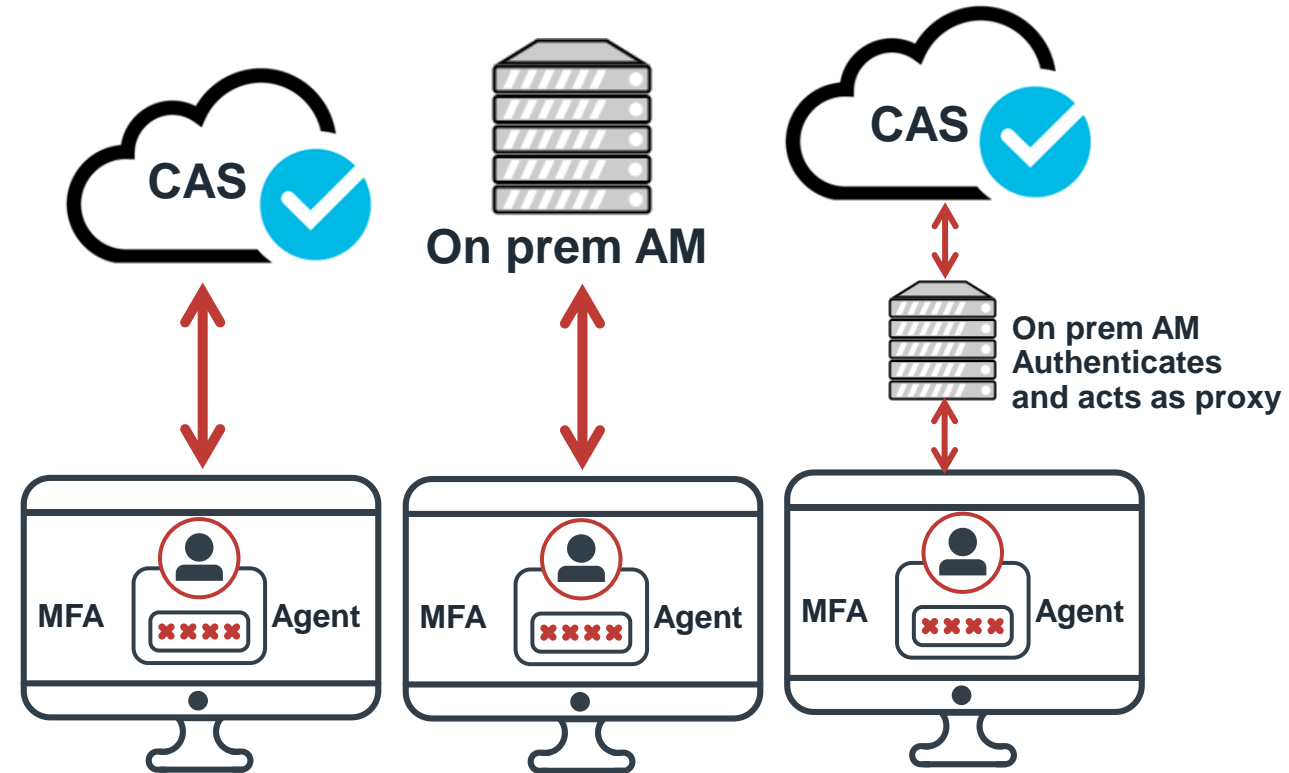
- **Communication Port:**

- AM => TCP 5555
- CAS => TCP 443

- **Components used for communication:**

- AM- CAS

- **Test Authentication:** MFA Agent Test Authentication





# GPO Configurations for MFA Agent (CAS)

- Required policies to be enabled for the Agent to work:
  - Enable RSA Authentication

The screenshot shows the 'Enable RSA authentication' Group Policy Object (GPO) configuration window. The window has a title bar with the icon and text 'Enable RSA authentication'. Below the title bar are 'Previous Setting' and 'Next Setting' buttons. The main area contains three radio buttons: 'Not Configured' (selected), 'Enabled', and 'Disabled'. To the right of these is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with a text box containing 'Windows 8.1 or later or Windows Server 2012 R2 or later.'. At the bottom, there are 'Options:' and 'Help:' sections. The 'Options:' section is empty. The 'Help:' section contains text explaining the policy: 'Specifies if the Agent requires RSA additional authentication during Windows authentication. If the policy is enabled, then RSA is used during Windows authentication. If you do not configure or disable this policy, then RSA is not used during Windows authentication.' At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

- API KEY

The screenshot shows the 'RSA Authentication API Key' Group Policy Object (GPO) configuration window. The window has a title bar with the icon and text 'RSA Authentication API Key'. Below the title bar are 'Previous Setting' and 'Next Setting' buttons. The main area contains three radio buttons: 'Not Configured' (selected), 'Enabled', and 'Disabled'. To the right of these is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with a text box containing 'Windows 8.1 or later or Windows Server 2012 R2 or later.'. At the bottom, there are 'Options:' and 'Help:' sections. The 'Options:' section contains a text box with the label 'Enter the RSA Authentication API Key.'. The 'Help:' section contains text explaining the policy: 'Specify the RSA Authentication API Key that the Agent sends to the RSA Authentication API to securely identify authentication requests. If you are connecting to the Cloud Authentication Service, the key is available in the Cloud Administration Console > My Account > Company Settings page. If you are connecting to Authentication Manager, the key is available in the Security Console > Setup > System Settings > RSA Authentication API page.' At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

# GPO Configurations for MFA Agent (CAS)

- Required policies to be enabled for the Agent to work:

- API REST URL

RSA Authentication API REST URL

Previous Setting Next Setting

☒ Not Configured ☐ Enabled ☐ Disabled

Comment:

Supported on: Windows 8.1 or later or Windows Server 2012 R2 or later.

Options:

Enter the RSA Authentication API REST URL.

Help:

Specify the RSA Authentication API REST URL to connect the Agent with RSA.

Specify the API URL using the following format:

https://hostname:port/

If you are connecting to the Cloud Authentication Service, the hostname is the Authentication Service Domain specified in the Cloud Administration Console. The default port is 443.

If you are connecting to RSA Authentication Manager, the host name is the Fully Qualified Domain Name specified in the Operations Console. The default port is 5555. You can enter up to 15 comma-separated URLs.

For more information, see the Group Policy Object Template Guide.

OK Cancel Apply

- Cloud Authentication Service Access Policy Name

Cloud Authentication Service Access Policy

Previous Setting Next Setting

☒ Not Configured ☐ Enabled ☐ Disabled

Comment:

Supported on: Windows 8.1 or later or Windows Server 2012 R2 or later.

Options:

Enter the exact name of the access policy as specified in the Cloud Administration Console.

Help:

Specifies the Cloud Authentication Service access policy to use to control which users can sign in with the Agent and how those users must sign in.

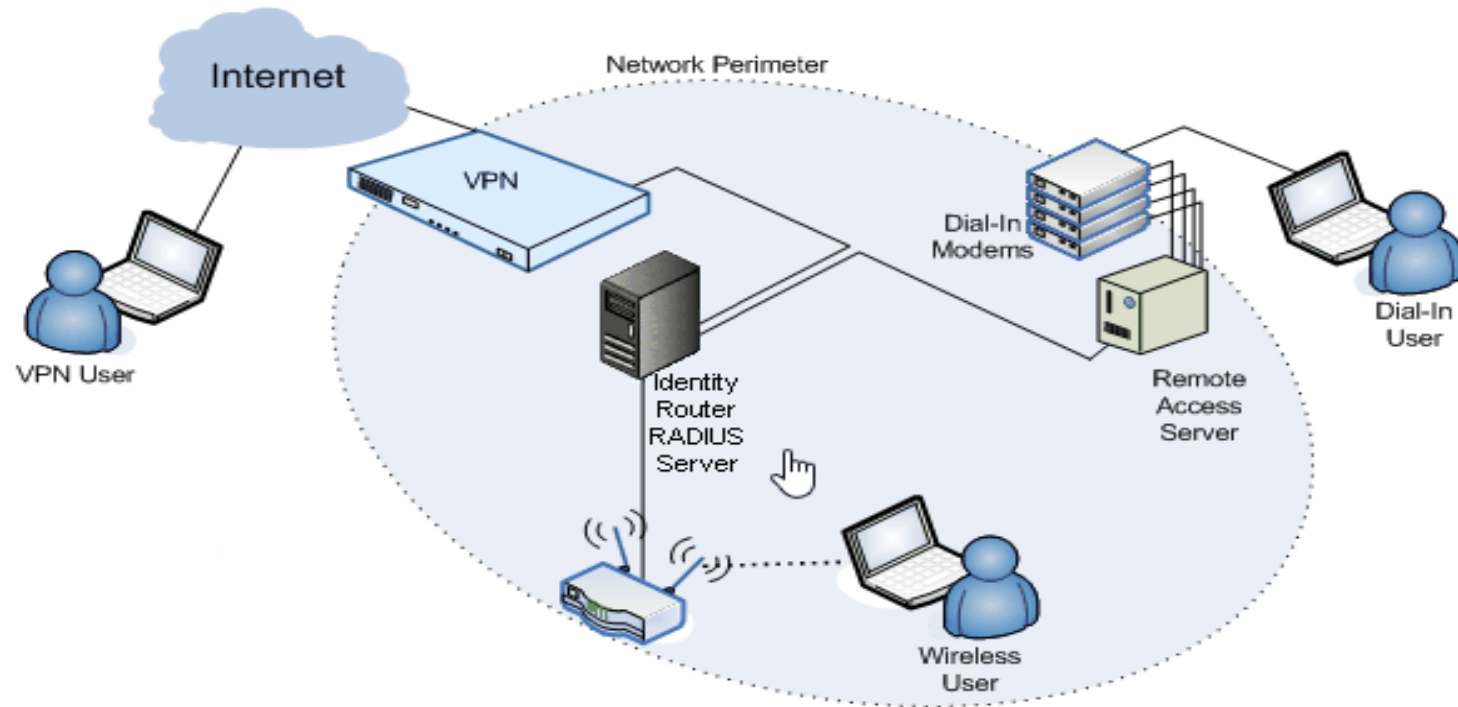
The available access policies are displayed in the Cloud Administration Console Access > Policies page.

OK Cancel Apply

# RSA

# RADIUS

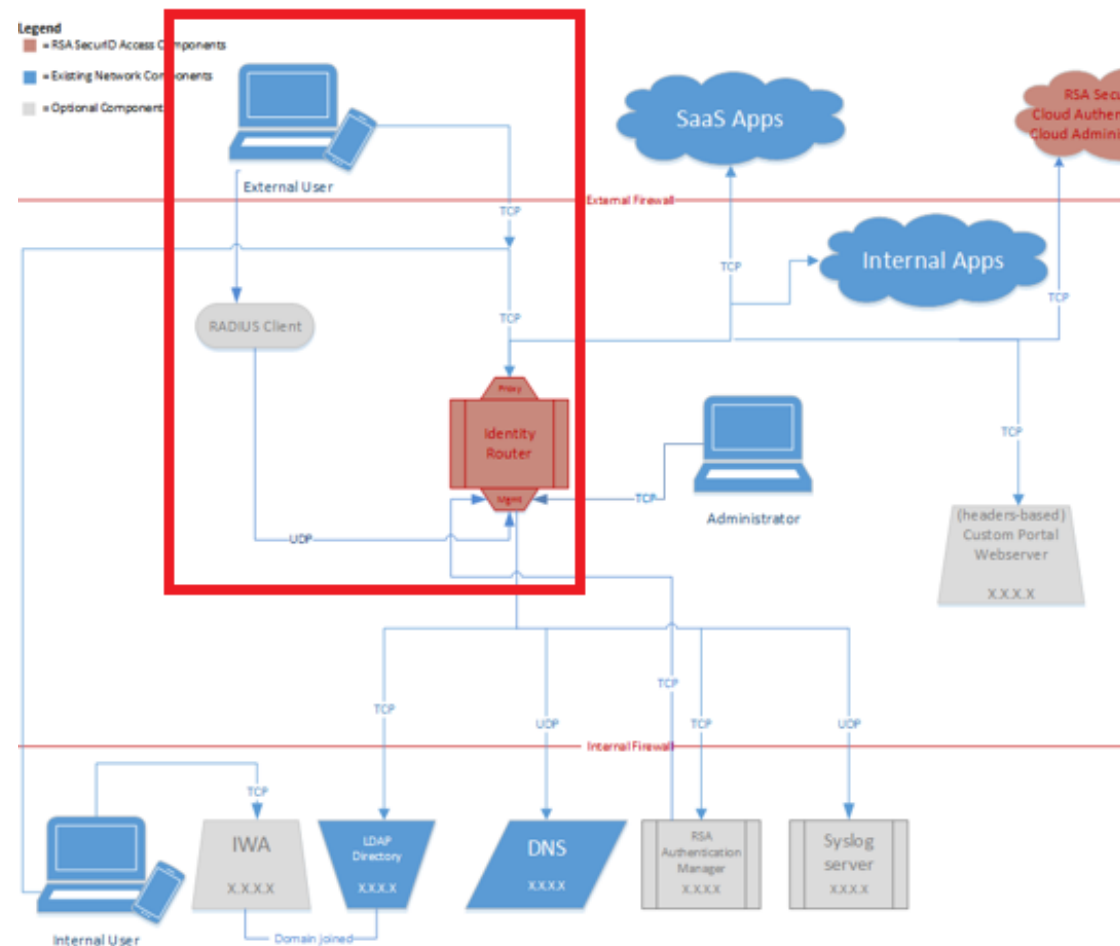
# High-Level Authentication Flow for RADIUS for the Cloud Authentication Service





# RADIUS

- Based on **FreeRADIUS server** IDR  
Management interface is the radius server
- Shared Secret is the main component
- Two main entities:
  - 1) Radius Server
  - 2) Radius Client





# SAML

Security Assertion Markup Language



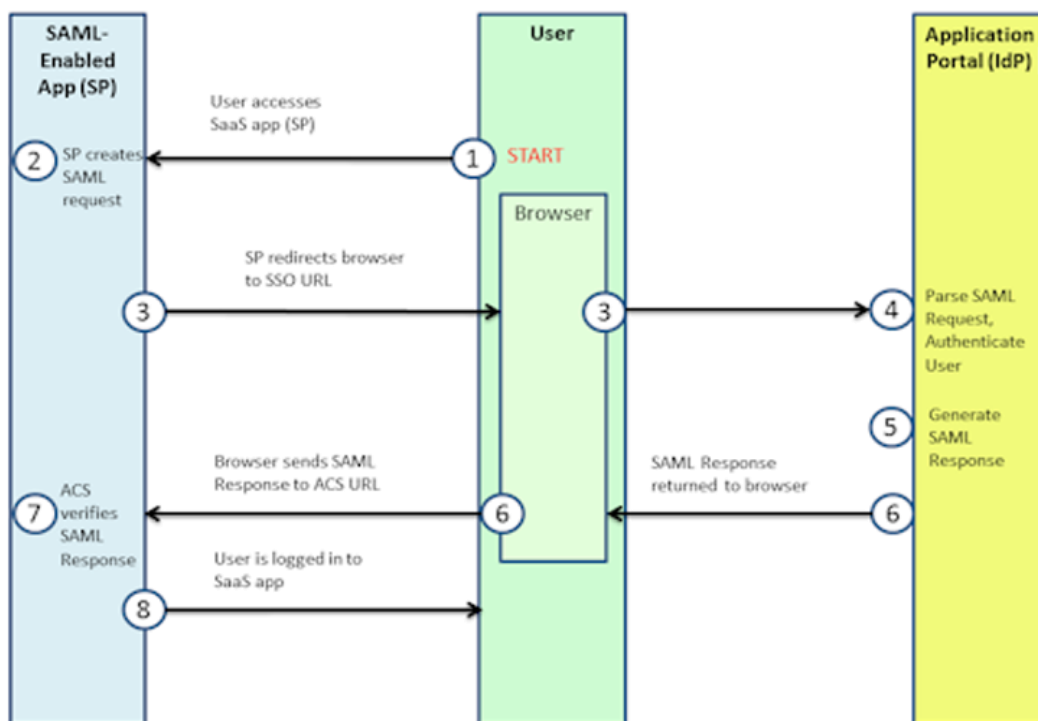
# Introduction

- SAML stands for Security Assertion Markup Language
- Open standard for authentication and authorization between different entities with an established trust
- Typically, one entity is the Service Provider (SP) and the other is the Identity Provider (IdP)

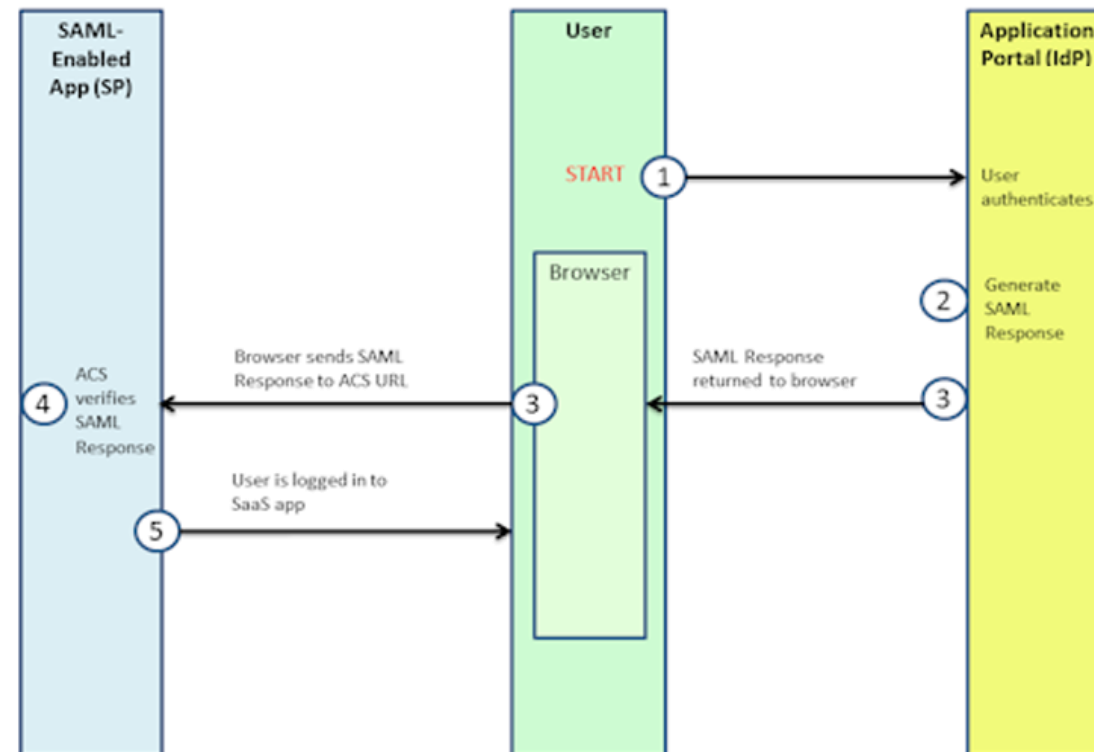
# SAML

- Typically, one entity is the Service Provider (SP) and the other is the Identity Provider (IdP)

## Communication Flow (SP-initiated and IdP-initiated)



SP-initiated/Relying Party



IdP-initiated





# SAML

SP Parameters



# SP Parameters – Entity ID

- Globally unique identifier used to identify the SP participating in the SAML authentication and authorization protocol
- Can be referred to as **Audience**, or **SP Identifier**
- Can be a URL or a string

# SP Parameters – Assertion Consumer Service URL

- Critical component of a SAML workflow to determine the direction of flow from the IdP to the SP
- Parses the Assertion to determine user access (grant/revoke)
- Must be unique and accessible

# SP Parameters – Connection URL

- Can be referred to SSO/Login URL
- For SP-initiated applications, this is the mandatory Endpoint that triggers the SAML request to the IdP
- For IdP-initiated applications, this is an optional Endpoint that acts as a Relay State to land the users on a specific SP page



# SP Parameters – NameID

- Another critical component of a SAML workflow
- Uniquely identifies the user accessing the SP
- Formats:
  - Auto Detect
  - urn:oasis:names:tc:SAML:2.0:nameid-format:entity
  - urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
  - urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
  - urn:oasis:names:tc:SAML:2.0:nameid-format:transient
  - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
  - urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

# SP Parameters – Signing Certificate (Optional)

- Some SPs require to have the requests signed (WantAuthnRequestsSigned=true)
- For a proper flow and the Assertion to be issued, the SP Signing Certificate must be present in the IdP configuration

## Message Protection

SAML Request Protection ⓘ

☐ SP signs SAML requests






No certificate loaded

Choose File

# SP Parameters – Attribute Statements (Optional)

- Some SPs require additional Attributes bound to users authenticating beyond their NameID

Statement Attributes ⓘ

Attribute Name	Attribute Source	Property		
<input type="text" value="LastName"/>	<input type="text" value="Identity Source"/>	<input type="text" value="sn"/>		
<div> ADD</div>				

- The Attribute can be constant or fetched from the configured Identity Source



# SAML

IDP Parameters





# IdP Parameters – Entity ID

- Globally unique identifier used to identify the SP participating in the SAML authentication and authorization protocol
- Can be referred to as **Audience**, or **IdP Identifier**
- Can be a URL or a string

# IdP Parameters – Service URL

- Uniquely identifies the IdP Endpoint the SP will send the request to
- Can be referred to as **Identity Provider URL**
- Typically ends in **/sso/saml/\***

# IdP Parameters – Signing Certificate (Optional)

- It's mandatory to have the IdP sign outgoing Assertions or the whole response
- For the SP to validate the signature, the Signing Certificate must be present in the SP configuration

## SAML Response Protection

- ☒ IdP signs assertion within response
- ☐ IdP signs entire SAML response
- ☐ Override default signing key and certificate

Download Certificate



☒ Override default signing key and certificate



No private key loaded

Choose File

Generate Cert Bundle



No certificate loaded

Choose File

# IdP Parameters – Encryption Certificate (Optional)

- Some SPs require the IdP to encrypt the outgoing Assertions (WantAssertionEncrypted=true)
- The SP Encryption Certificate needs to be present in the IdP configuration

☐ Encrypt Assertion ⓘ



No certificate loaded

Choose File

Data Encryption Algorithm

AES 128 ▼

Key Encryption Algorithm

RSAOAEP ▼





# Q&A







# Thank you



