Module 6: Implement an Azure Active Directory

Understanding Active Directory

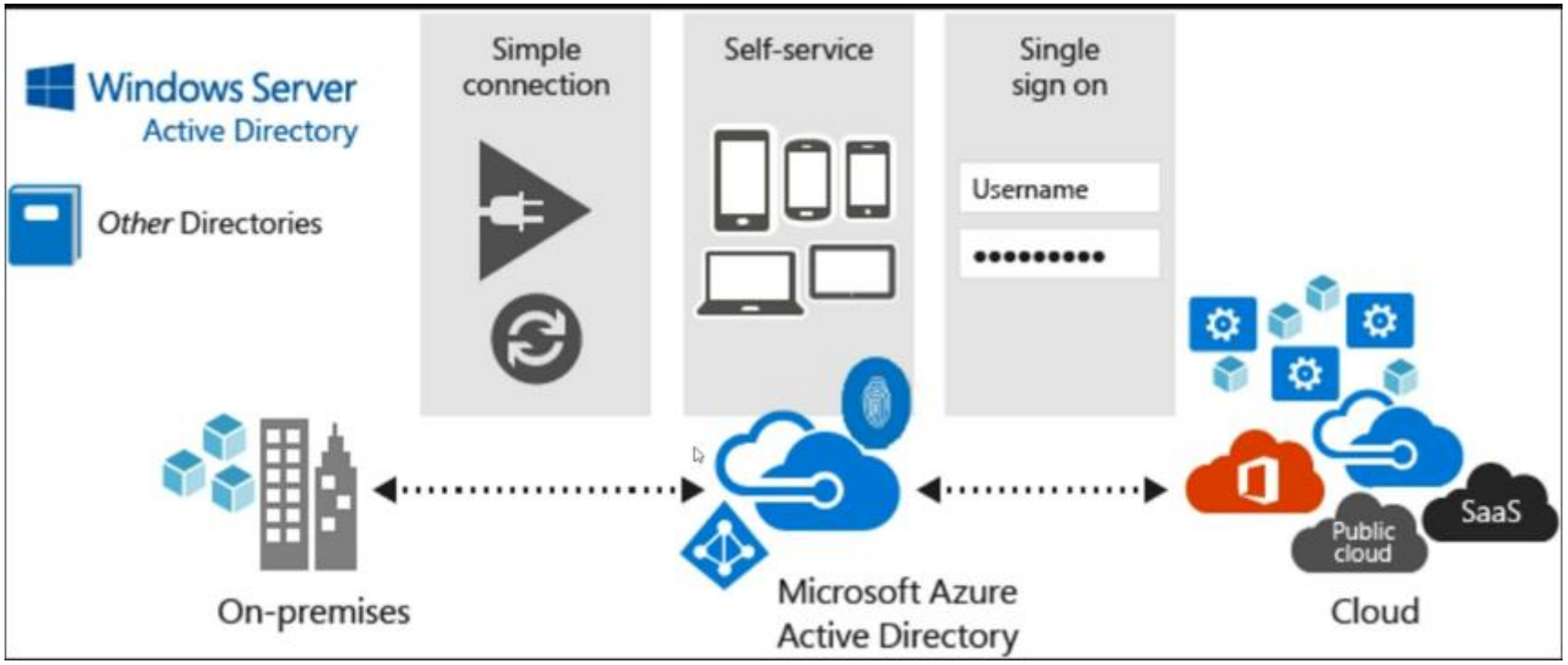
What is a Directory Service?

A service that helps track and locate objects on a network

- A directory service is a container that provides a hierarchical structure and allows to store objects for quick and easy access and manipulation. A directory service is like an electronic phone directory that lets you search for Name and retrieve the phone number, address, or other information without knowing where that person lives.
- Before directory services, If you needed a file, you needed to know the name of the file, the name of the server on which it is stored and its folder path. Now this works well on small network, but as the network grows it becomes challenging.
- Directory service is the means by which users and administrators can locate resources regardless of where those resources are located.
- Also earlier typical user could have more than one user account or password, and as the network grows and the number of username and password also increases, like one for File Server, one for email server, etc.

Active Directory

AD is a traditional Active directory than many company use to manage the people resources, computers and objects within their company. It allows you to have permissions and you sign on with your windows machine and it checks with the Active Directory Server to ensure that user have permissions. It uses protocol like LDAP and Kerberos which are establish network protocol for logging in, verification and authentication in a network.



- The primary database is the Directory Information Base (DIB), which stores information about the objects.
  Major limitation was its lack of integration with Internet Protocol (IP).
- Protocol it used was Directory Access Protocol, or DAP.
  DAP offered more functionality than that is required for implementing directory services,
  so a scaled down version called Lightweight Directory Access Protocol (LDAP) was made.
  Later it was considered as a standard by Internet Engineering Task Force (IETF).
- LDAP relies on the TCP/IP stack rather than the OSI stack
- Integrate with IP and enable IP clients to use LDAP to query directory services.
- LDAP can perform hyper-searches.
  Giving one directory the ability to defer to another to provide requested data.
- LDAP supports Kerberos authentication, Simple Authentication Security Layer (SASL),
  and Secure Sockets Layer (SSL)
- Simple Authentication and Security Layer (SASL) is a framework for authentication
  and data security in Internet protocols.

More on Active Directory....

- AD is Microsoft's answer to directory services and it does a lot more than just locating resources.
- AD uses LDAP as its access protocol.
- AD relies on DNS as its locator service, enabling clients to locate domain controllers through DNS queries.

Naming Conventions

- AD contains information about objects in your enterprise.
- These objects can be computers, users, printers etc.
- AD is a container with nested containers holding other containers or objects.
- And we name these container and objects so that its easy to query or search.

Two types of Naming Convention

- User Principal Names, or UPN
- LDAP names also known as Distinguished Name

User Principal Names, or UPN

- This one you'll probably find most familiar, is as per RFC 822 specification.
- This has the same format as your email address: Like user@xyz.com
- They take the form user@domain
- If you have a user named User01 under Active Directory domain Domain01.local, the UPN will be User01@Domain01.Local
- We will discuss more about AD domain later.
- In AD you can create custom UPNs too, which means you can also add User01@Domain01.com or User01@xyz.com as UPN for above mentioned object.

LDAP names also known as Distinguished Name

- Typically it has this format
  - cn=common name
  - ou=organizational unit
  - dc=domain
  - cn=User,ou=Engineer,dc=xyz,dc=com
- And if you query for the
  - LDAP://XYZ01.road2master.ms/cn=User,ou=Engineer,dc=xyz,dc=com

Active Directory objects

◦Objects in AD can be either containers for other objects or they can be leaf objects, which do not serve as containers.
◦Objects in AD have attributes, and these attributes not only define the object but also store data. This defines the character of that Object.
◦Some attributes and optional and some are mandatory.
◦Optional : Phone Number
◦Mandatory: Username

Domain, Tree and Forest

AD Domain
Objects that are made on AD are grouped into domains.
The objects for a single domain are stored in a single database (which can be replicated).
AD Domain Tree
A tree is a collection of one or more domains
AD Forest
A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration.

What is Azure AD?

Extension of AD to the cloud

Synchronized copy of AD

Modern authentication protocols

WS-Federation

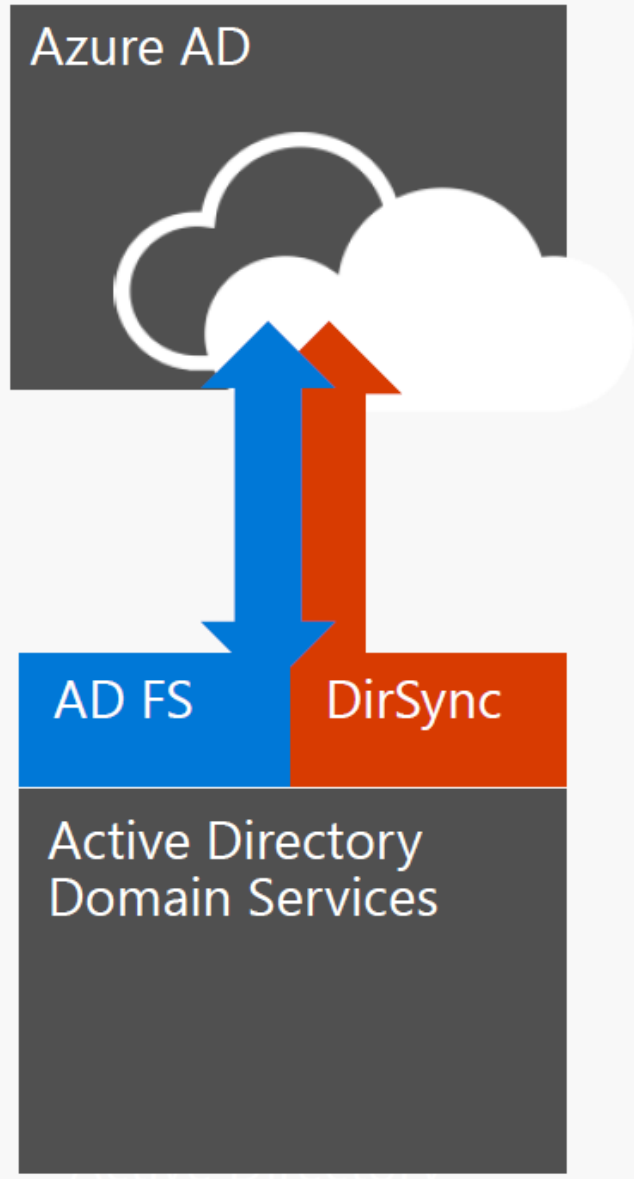
SAML 2.0

OAuth 2.0

OpenID Connect

Graph API for directory lookups

REST API for CRUD operations

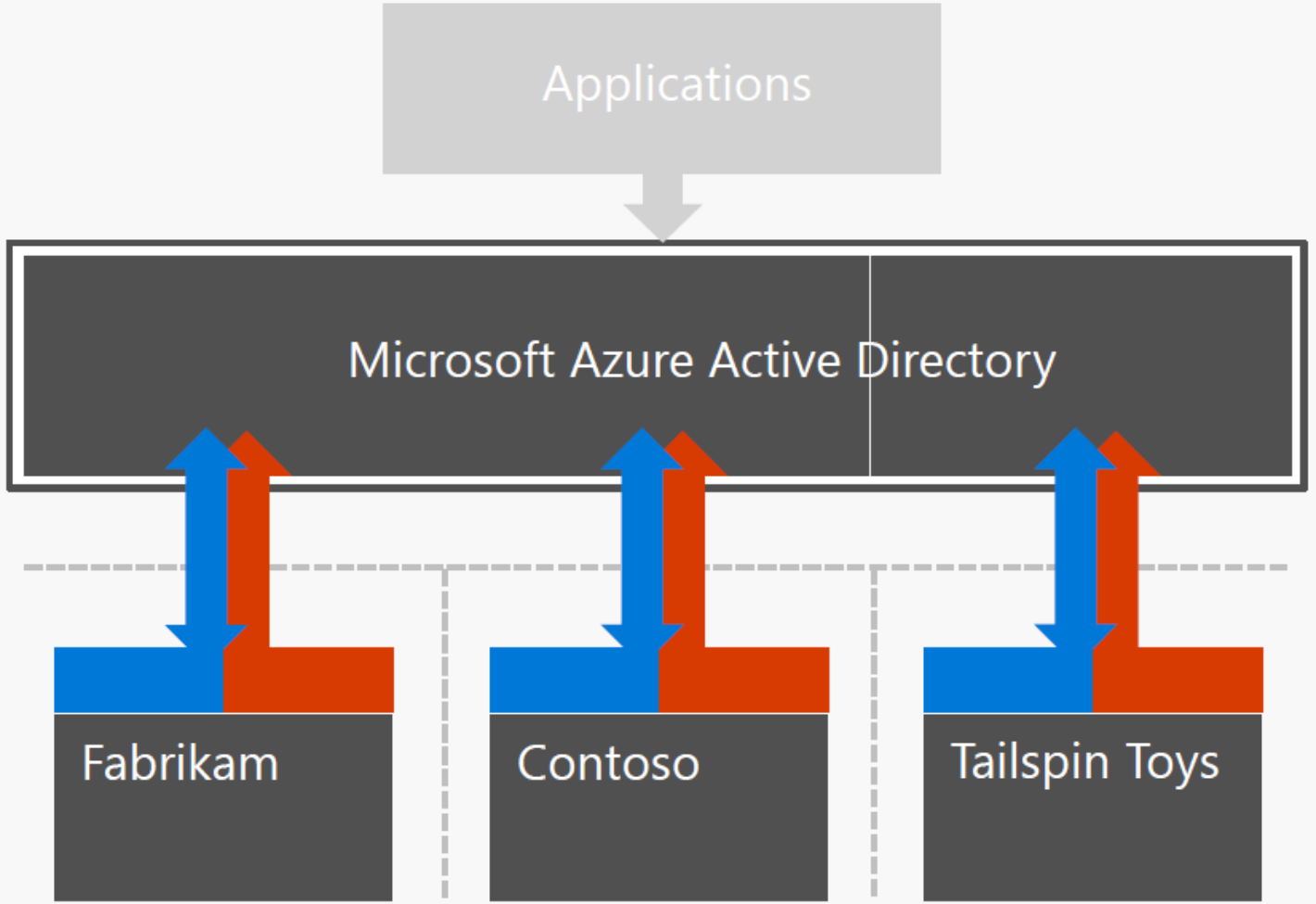


Multi-tenant identity service

Identity marketplace for applications

- Common endpoints
- Common signing certificate
- Customer control for trusted applications

Identity across organizational boundaries

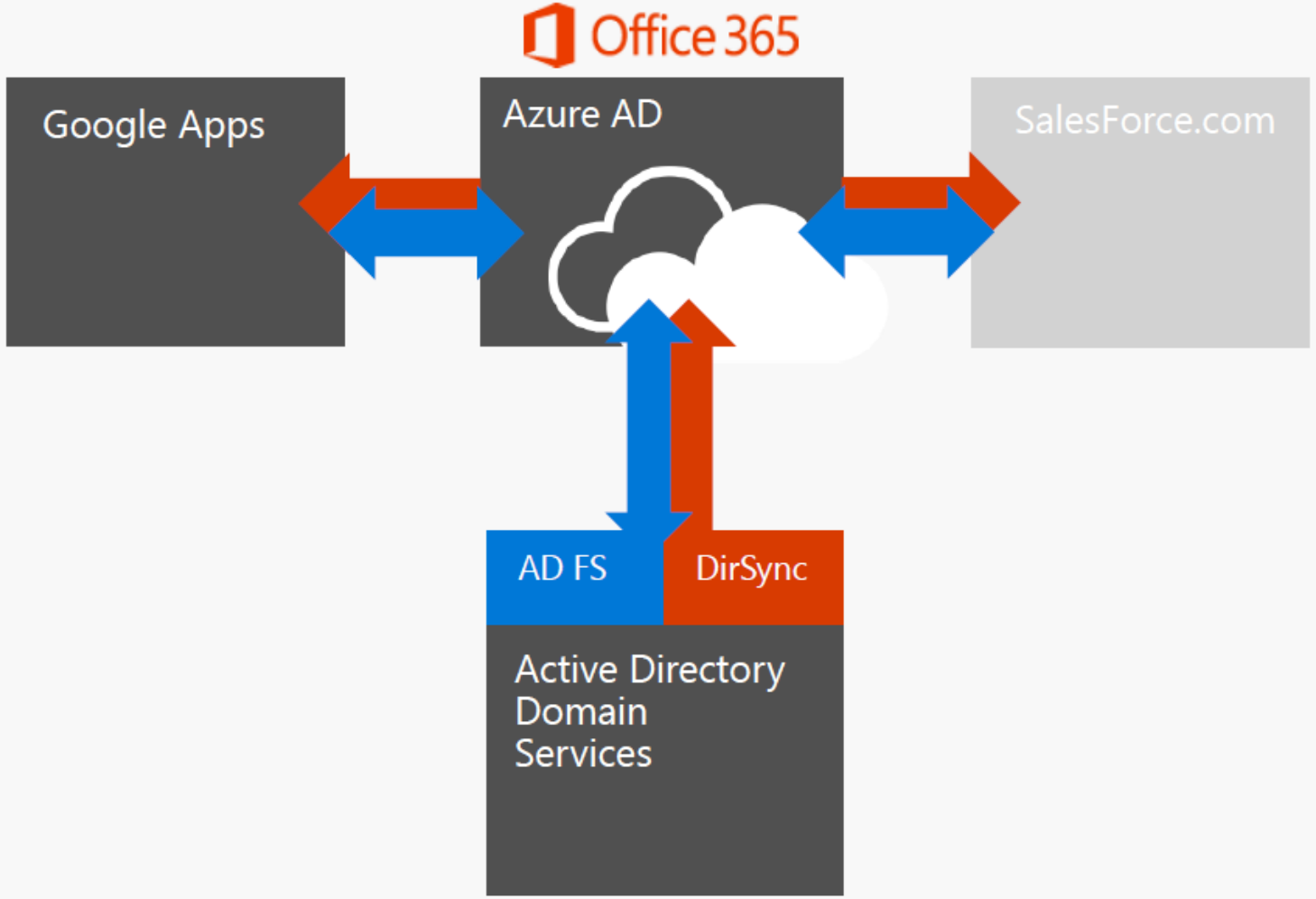


Identity management as a service

Identity services in the cloud

- Synchronization and SSO for third-party SaaS applications
- Application access panel
- Multi-factor authentication
- Self-service password reset

More on the way



Identity platform for MS online services

Facilitates authentication and provides directory information for:

- Office 365 (Exchange Online, Lync Online, SharePoint Online)
- Microsoft Dynamics CRM Online
- Microsoft Intune
- Azure Portal
- Azure Rights Management Services
- More and more all the time…

Any customer on Office 365 is already an Azure AD customer

Premium identity capabilities

Self service

SAAS app management

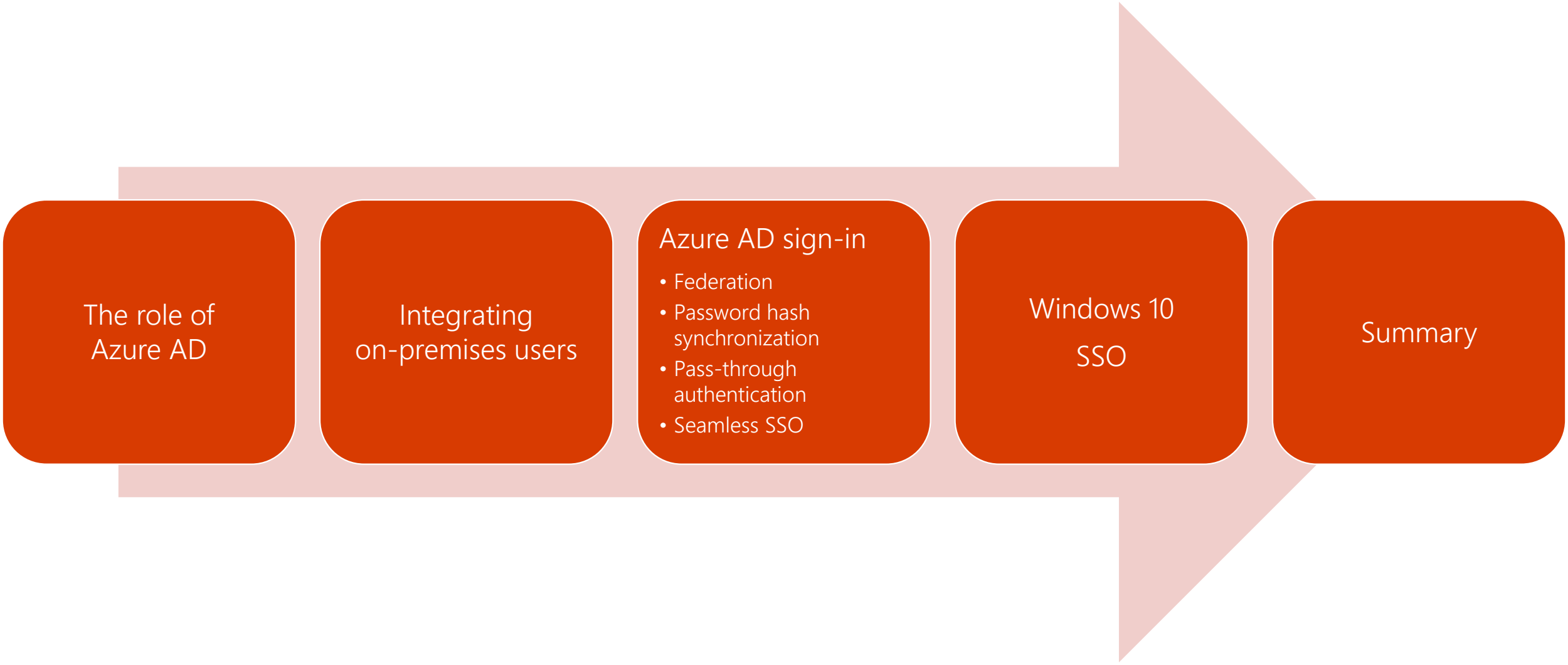
Multi-factor authentication

Azure AD intelligence

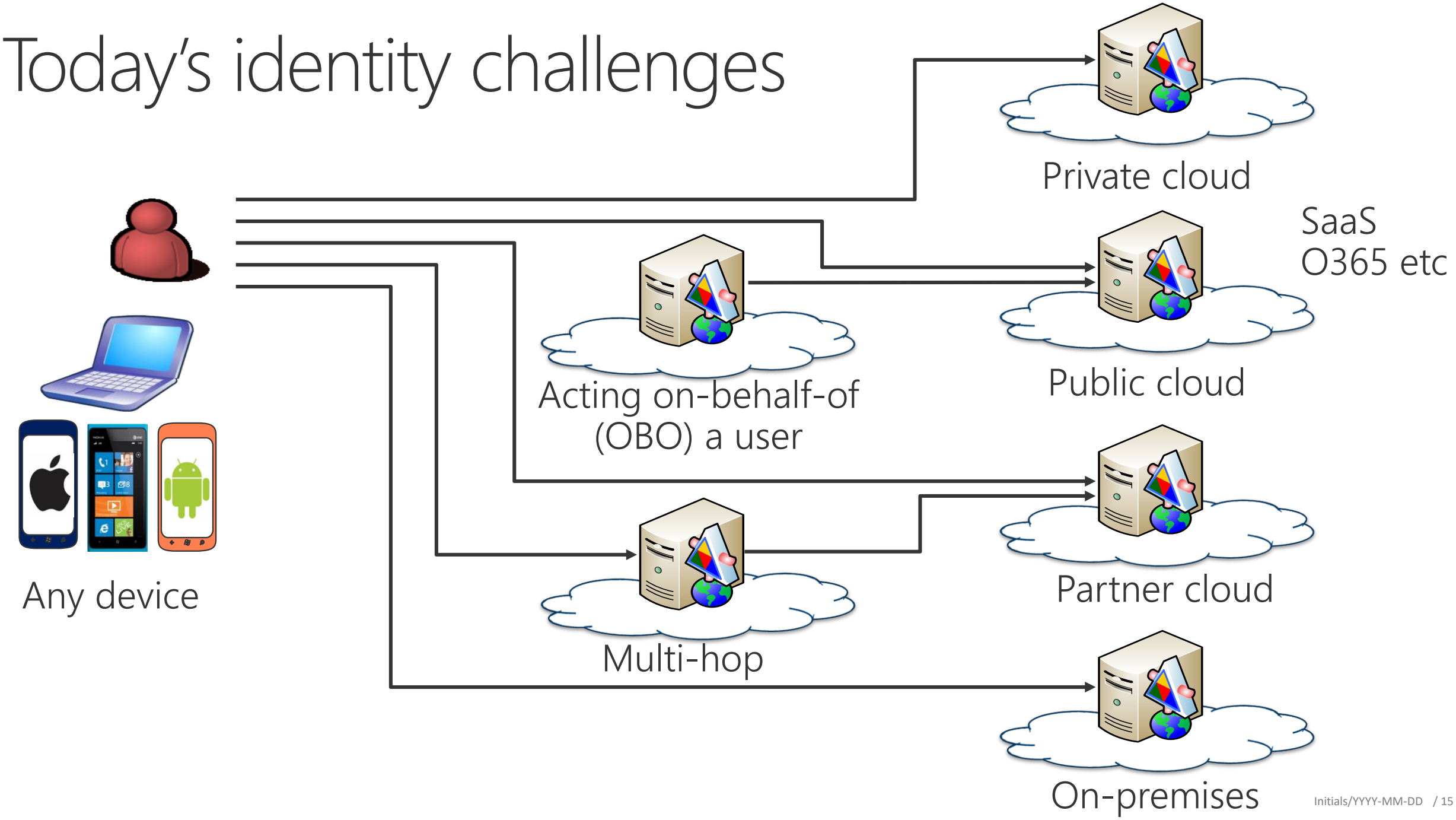
Administrative units

Azure AD Domain Services

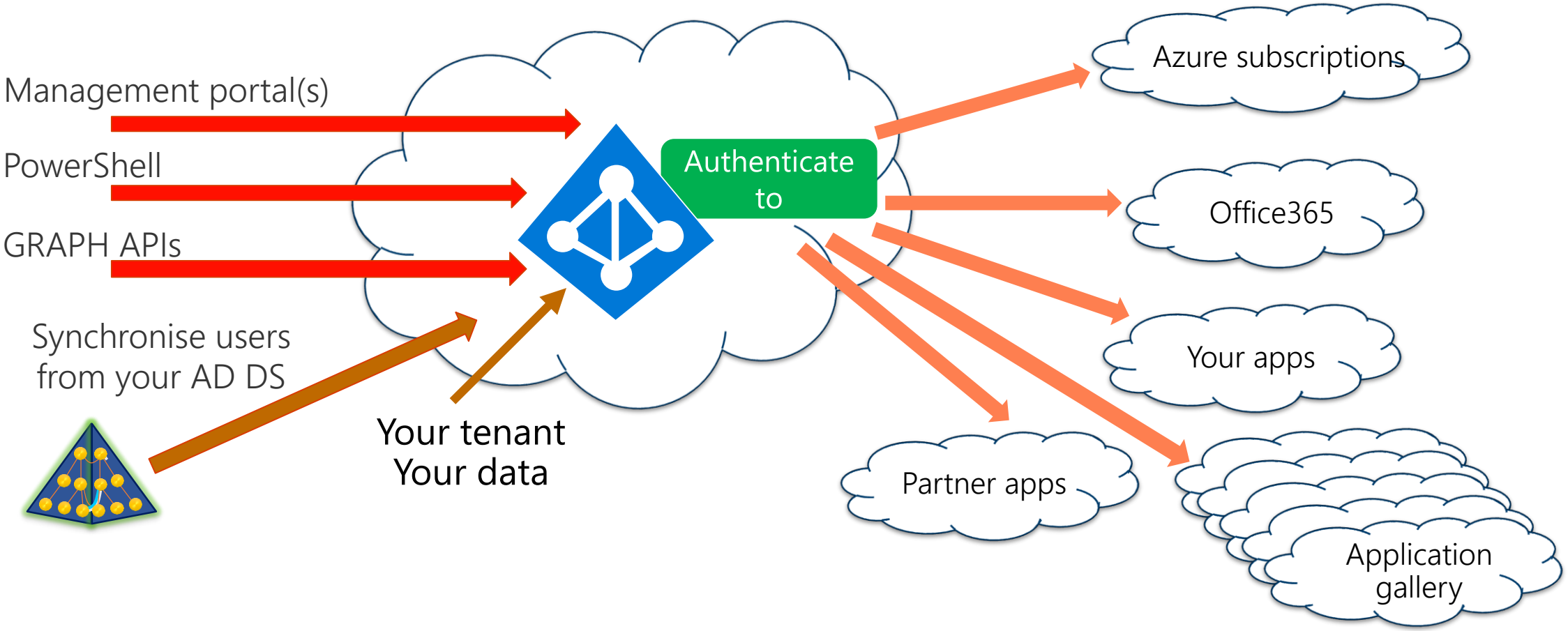
What's in this session



Today's identity challenges



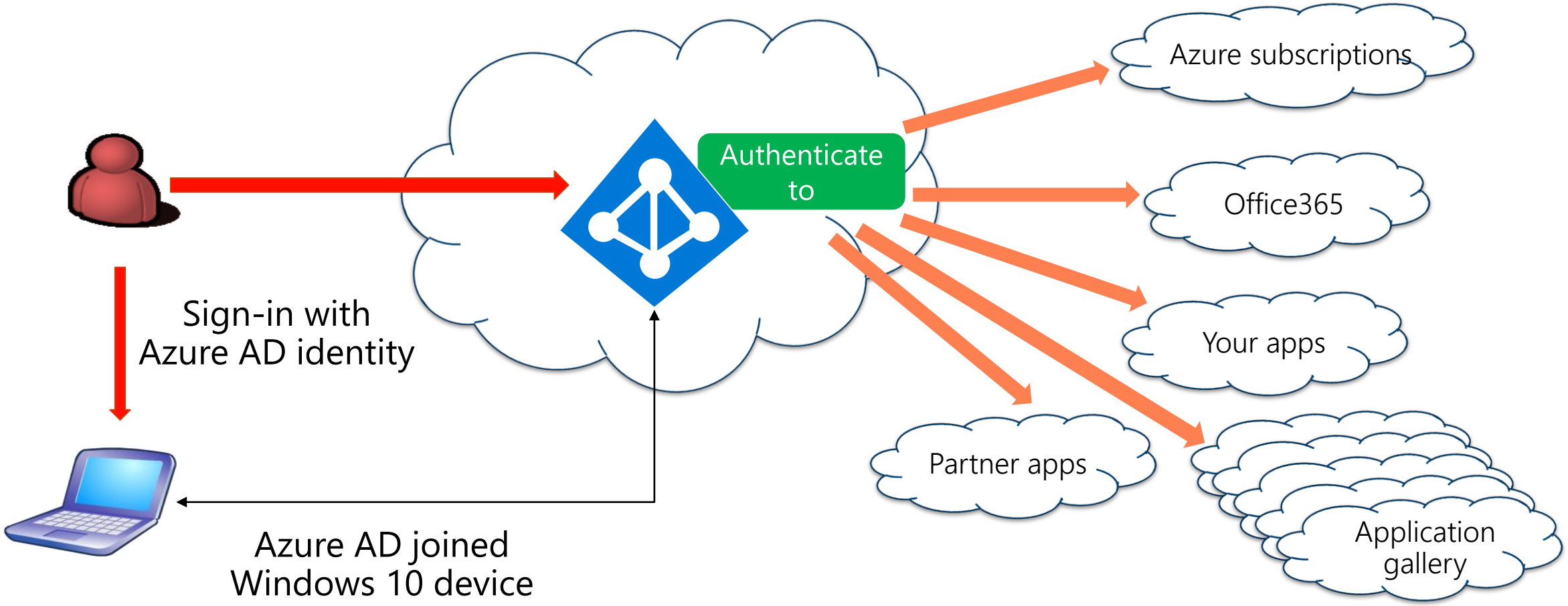
Microsoft Azure AD to the rescue



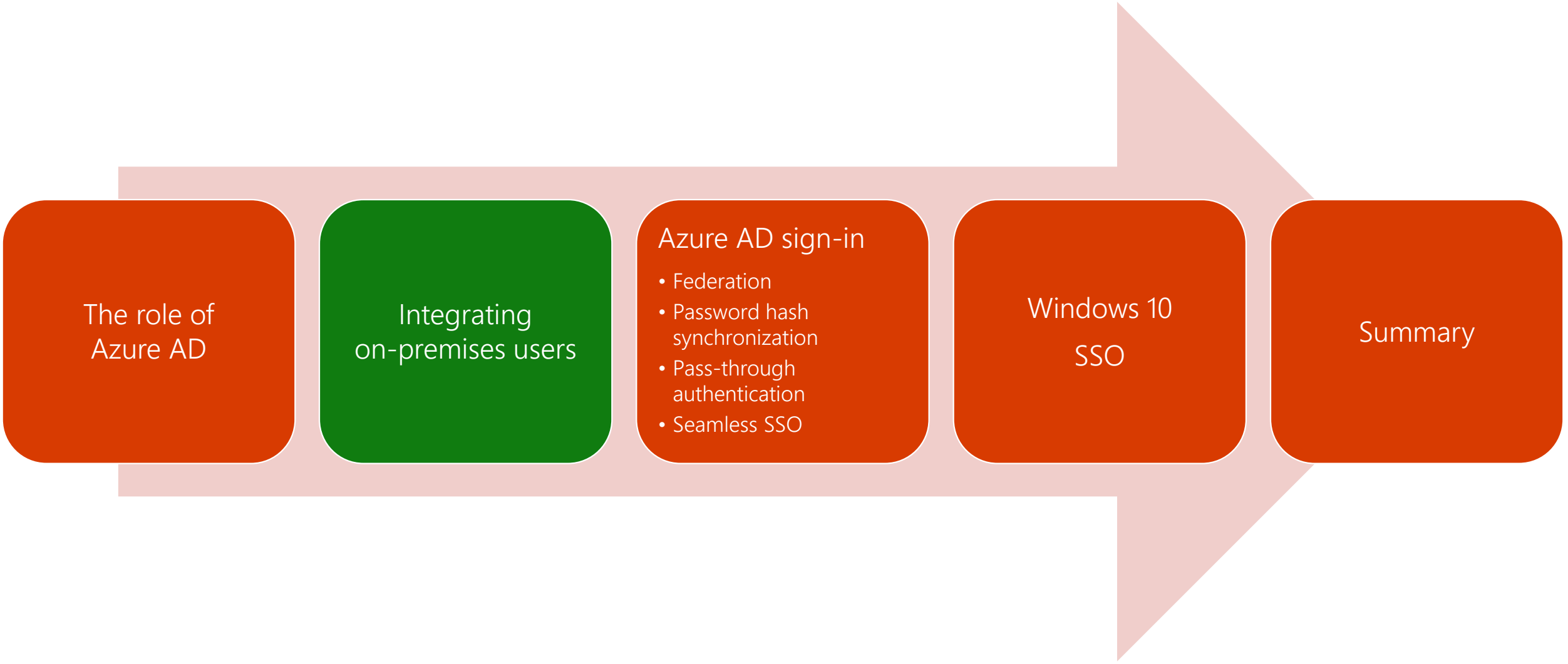
Azure AD benefits

- Authentication to applications via
  - OpenID Connect / Oauth 2.0
  - WS-Federation and SAML
  - Windows Kerberos Authentication via the Azure AD Application Proxy
- Self-service for
  - Password resets, application and group management
- MFA
- Conditional access
- Identity protection
- And more…

Cloud only user



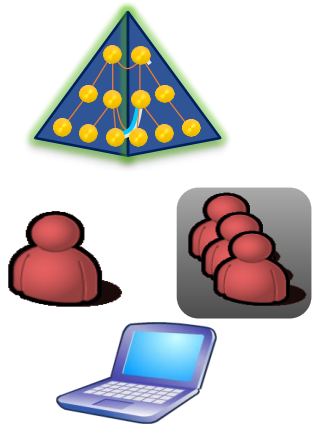
What's in this session



Unleash on-premises AD users

On-premises

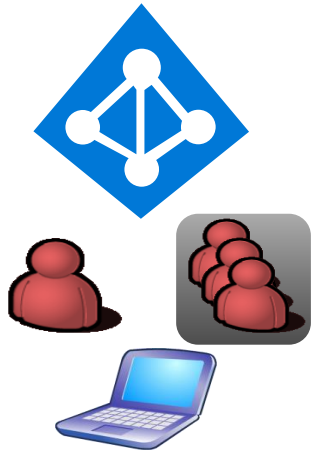
Azure AD



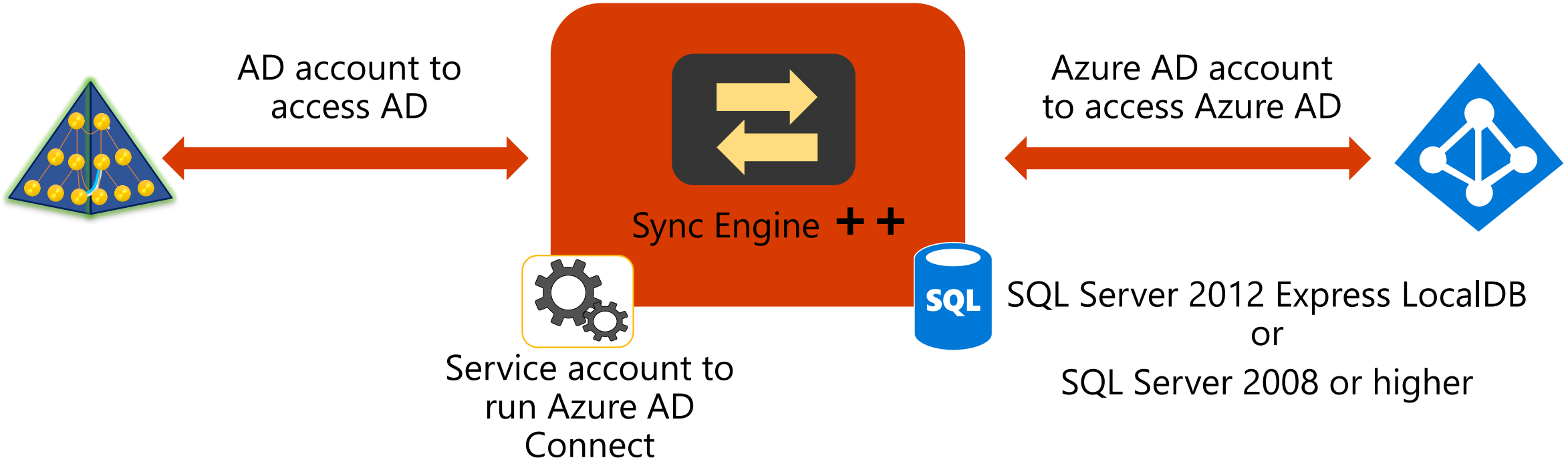
Synchronise users, groups and devices

Requires immutable ID

Enable write-back for passwords, devices and groups



Azure AD Connect

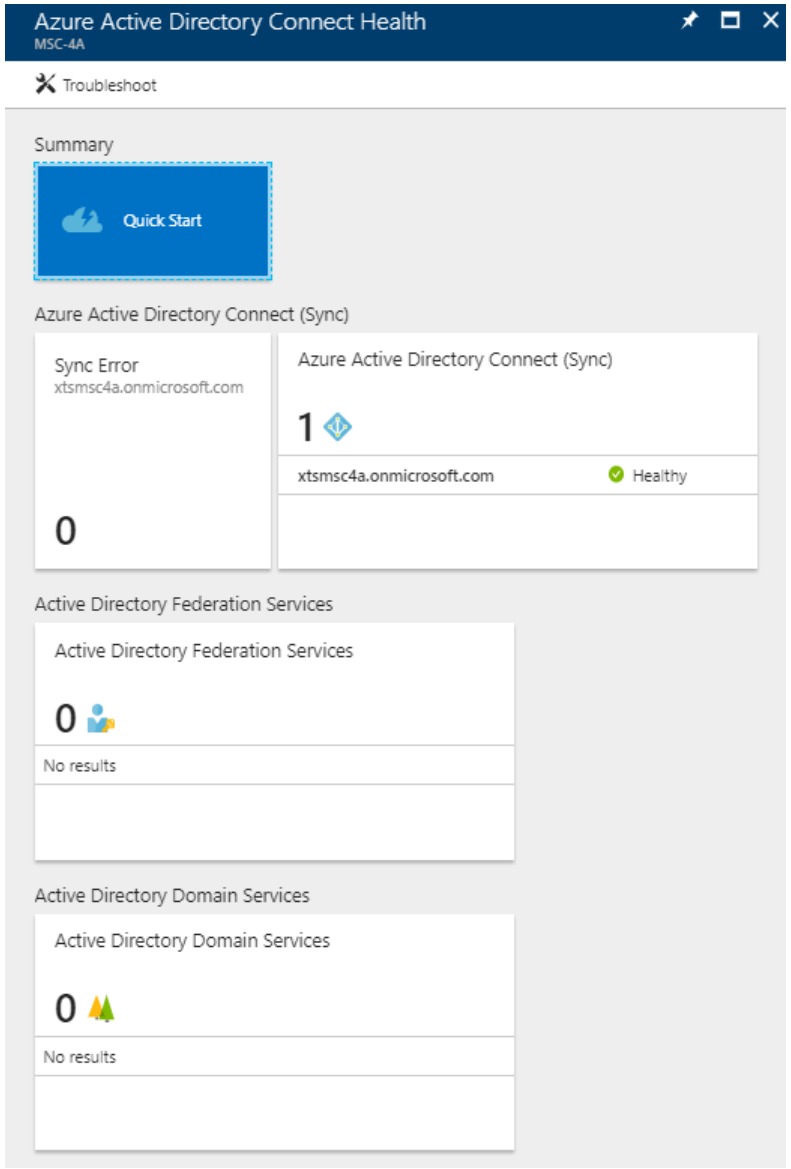


- Continuously evolving product
  - Automatic upgrades are possible
    - Set-ADSyncAutoUpgrade

Azure AD Connect

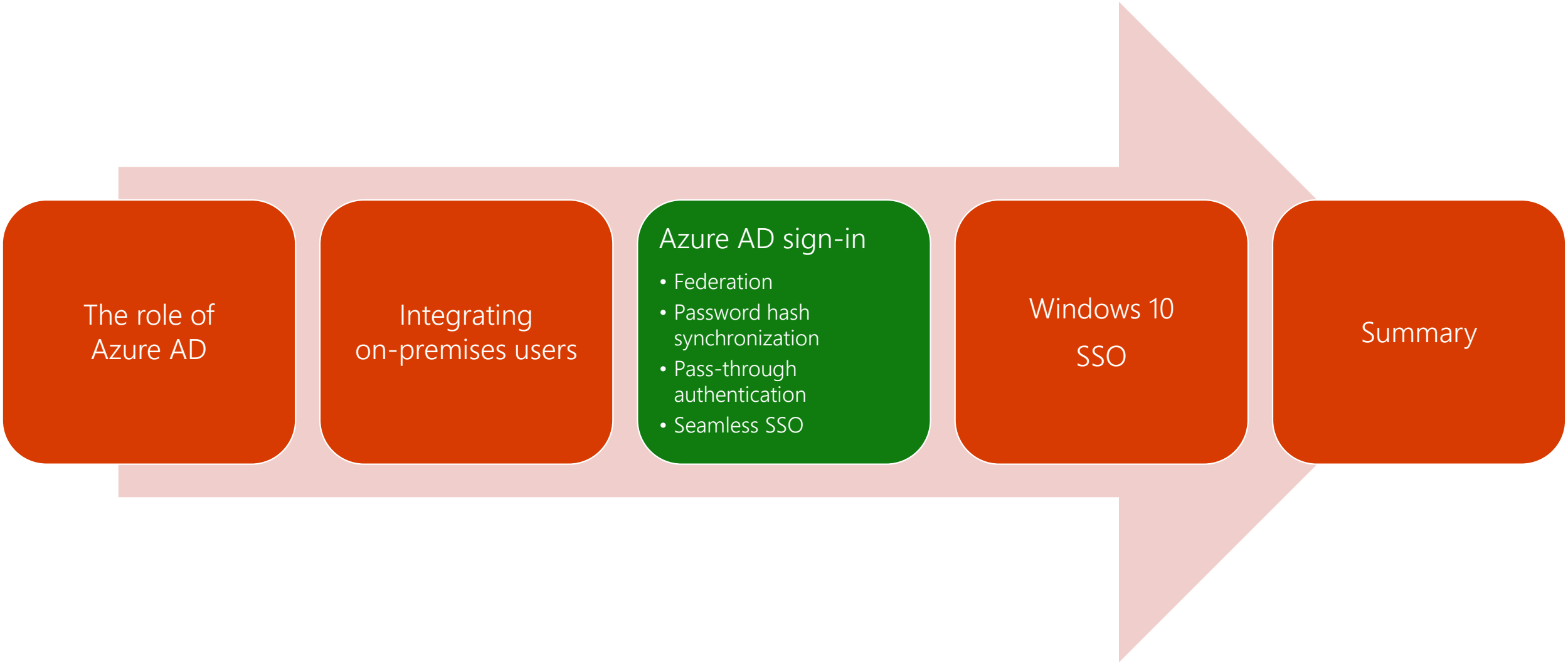
- AD Connect replaces earlier tools, upgrades are possible
  - DirSync
  - Azure AD Sync
  - FIM and the Azure AD Connector
- ++ more than just a synchronization engine
  - Manages user sign-in options
  - Write-back for password, devices and groups
  - Tools to support AD FS
    - Simple UI experience to update AD FS SSL certificates
    - Fix trust
    - Login testing
  - Azure AD Connect Health agent, reports status to the Azure AD Connect Health Portal

Azure AD Connect Health

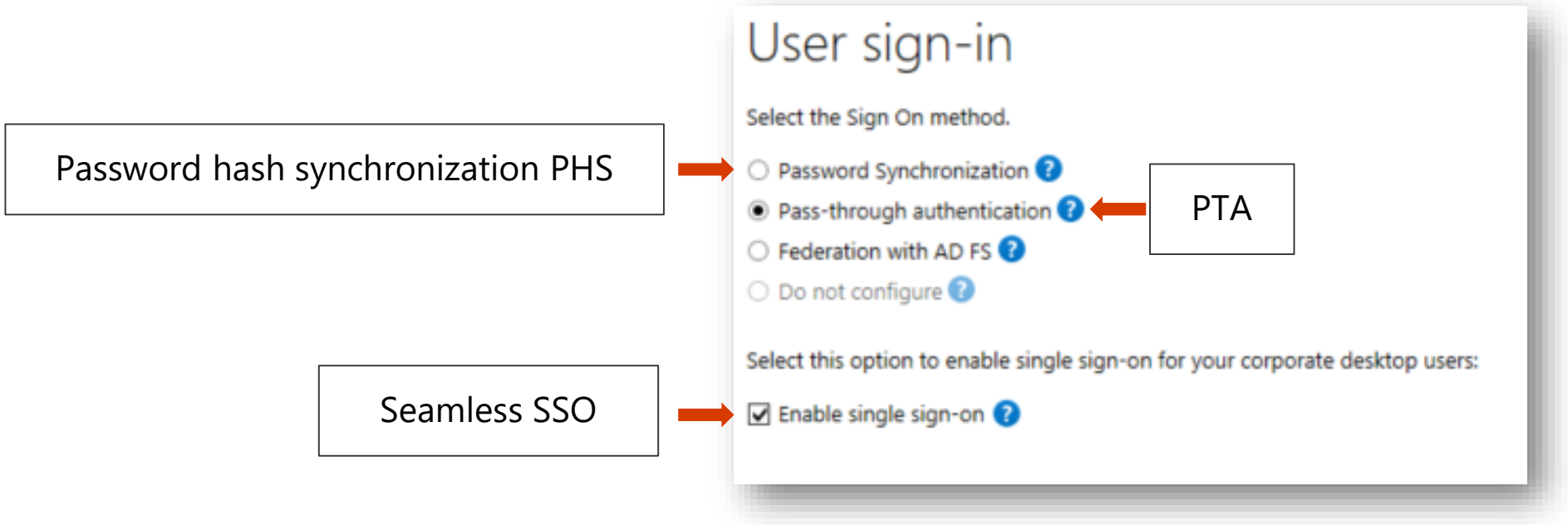


- One-stop shop for viewing the health of your identity infrastructure
  - Azure AD Connect
  - AD FS
  - On-premises AD
- Agents installed on identity infrastructure components
  - Monitoring and alerts
  - Email notification of critical alerts
  - Trends in performance data
  - Usage reports
- Requires a P1 license

What's in this session



Configuring Azure AD sign-in options



- The options defines how a synchronized on premises user signs in to Azure AD
  - "Do not configure" is used if a 3rd party federated solution is being used
- Seamless SSO works with PHS and PTA

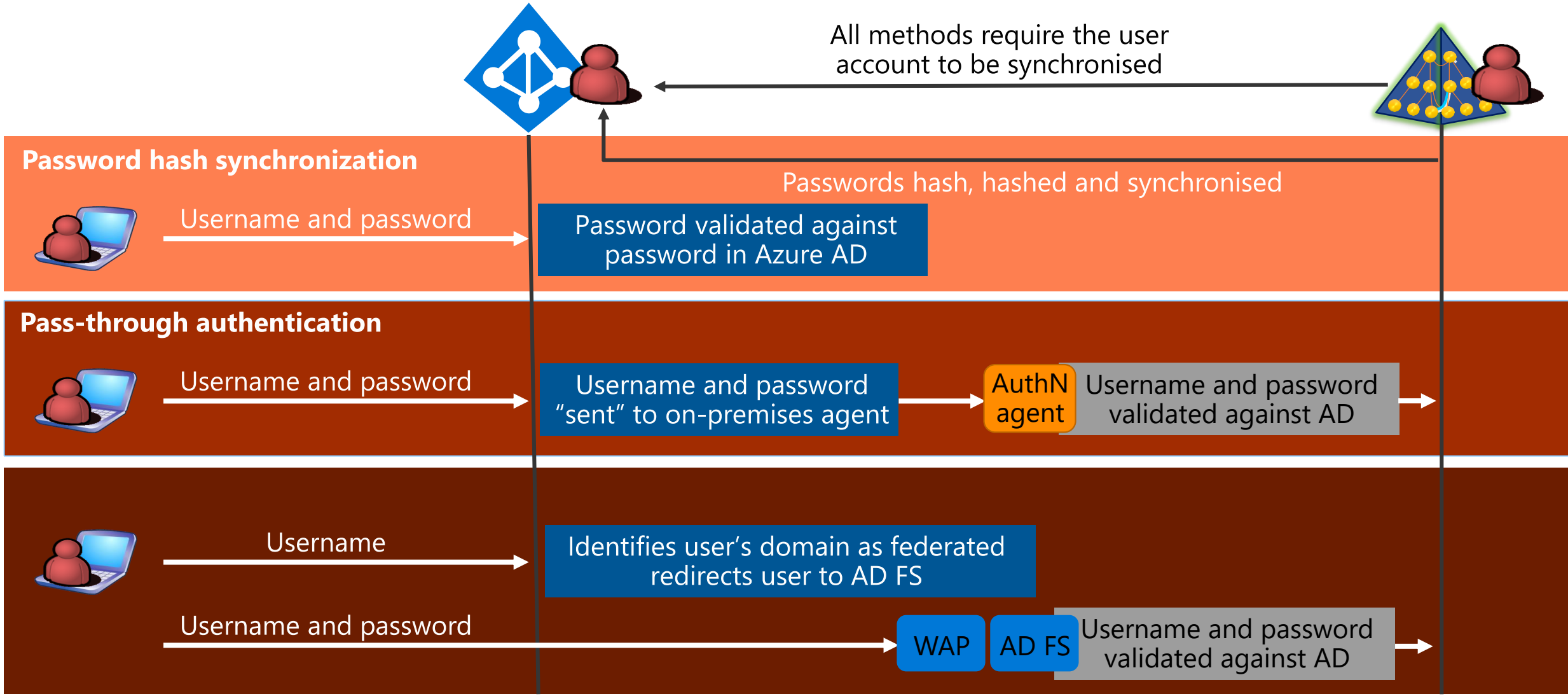
Managing on-premises passwords

- With PHS enabled, on-premises password changes synced to Azure AD within 2 minutes
- Password reset for on-premises passwords available via the Azure AD
  - Requires password writeback
  - Works for passwords reset by the administrator
  - Works for Self-Service Password Resets (SSPR)
  - Synchronous operation
  - Enforces on-premises password policies
  - Passwords for protected on-premises accounts cannot be reset

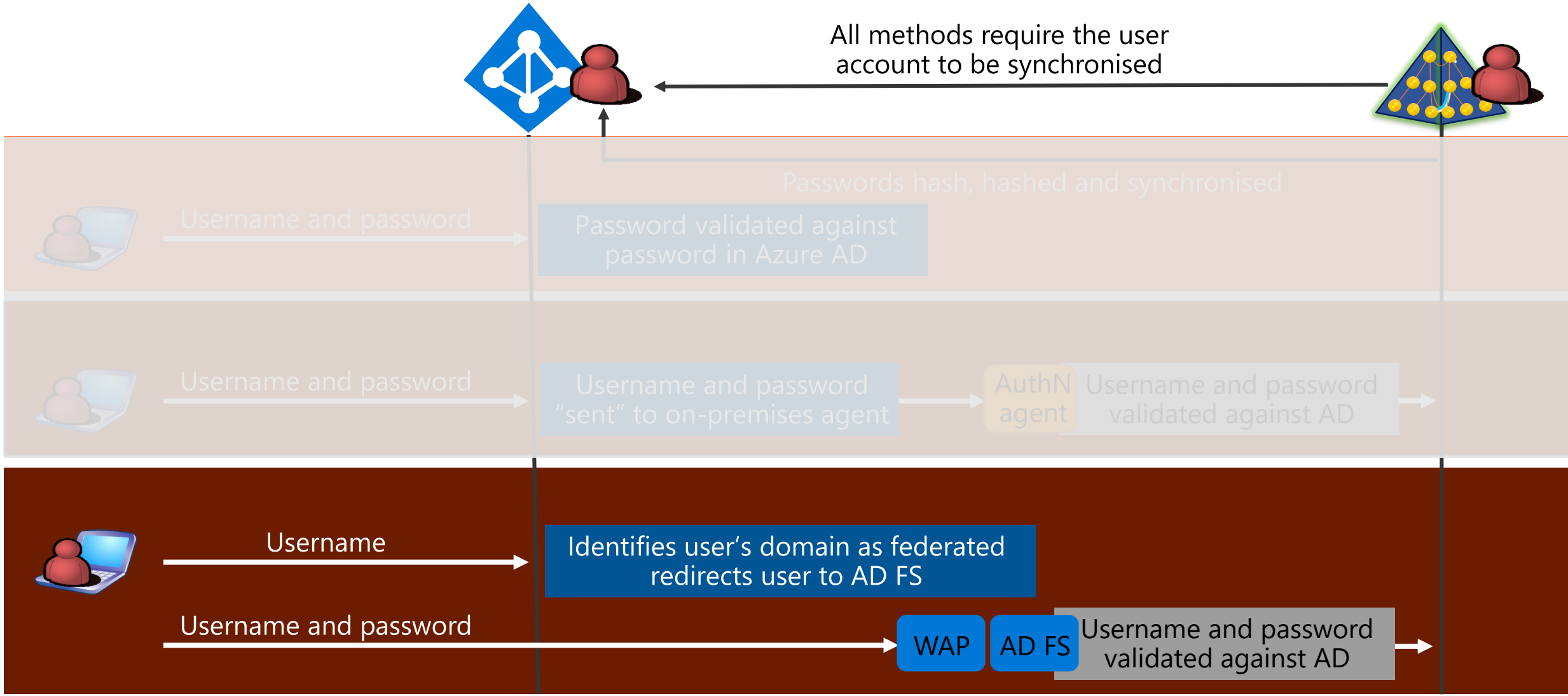
Azure AD sign in name

- The recommendation if for users to sign in to the Azure AD using their on-premises UPN
  - Provides maximum compatibility
  - Requires the on-premises UPNs to have verified DNS suffixes
    - Non verifiable UPN suffixes will need updating
- If the UPNs cannot be updated
  - Azure AD Connect can be configured to map a different on-premises attribute to the Azure AD UPN
    - It is recommended to use the mail attribute
    - Referred to as the Alternate ID

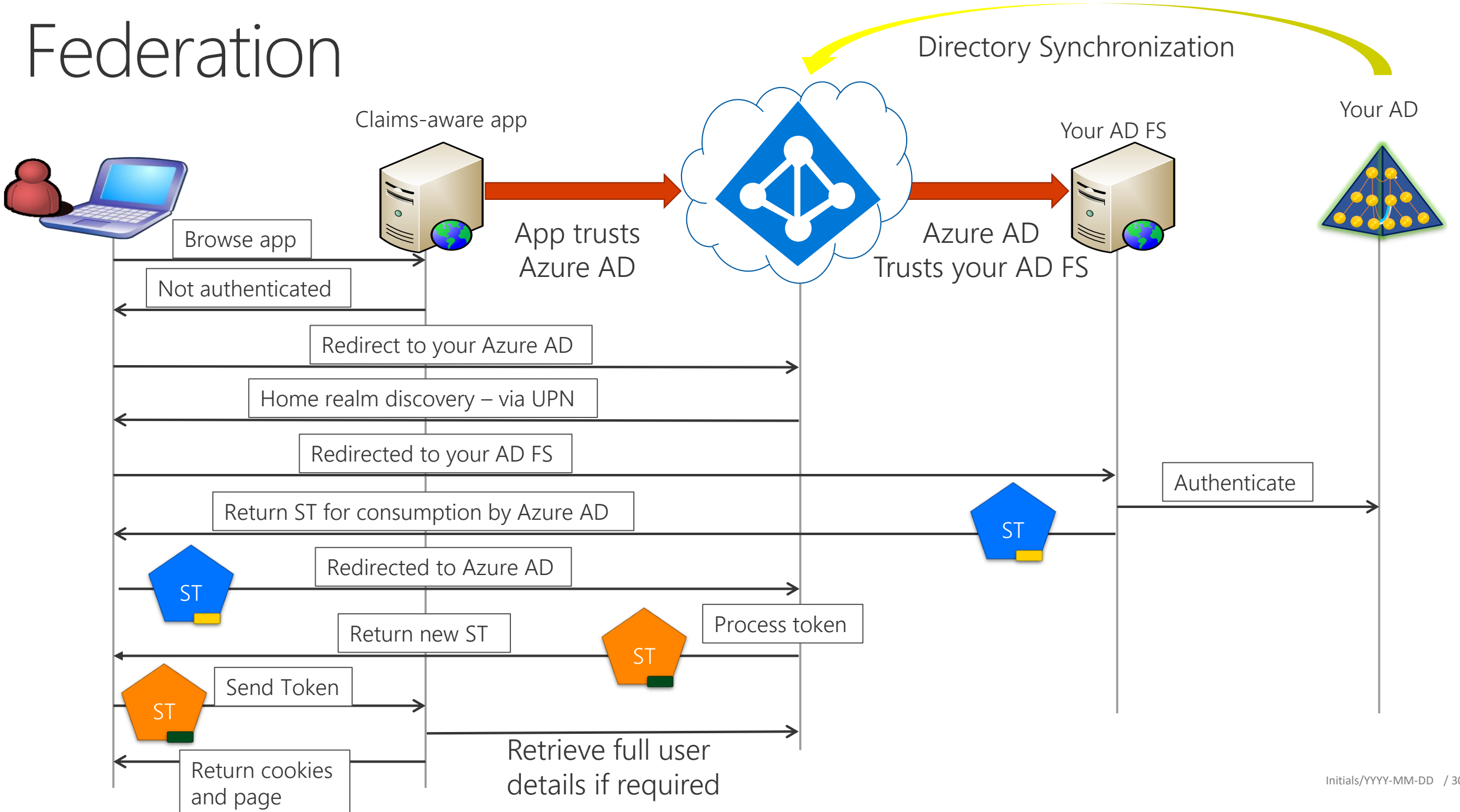
On-premises user sign-in to Azure AD



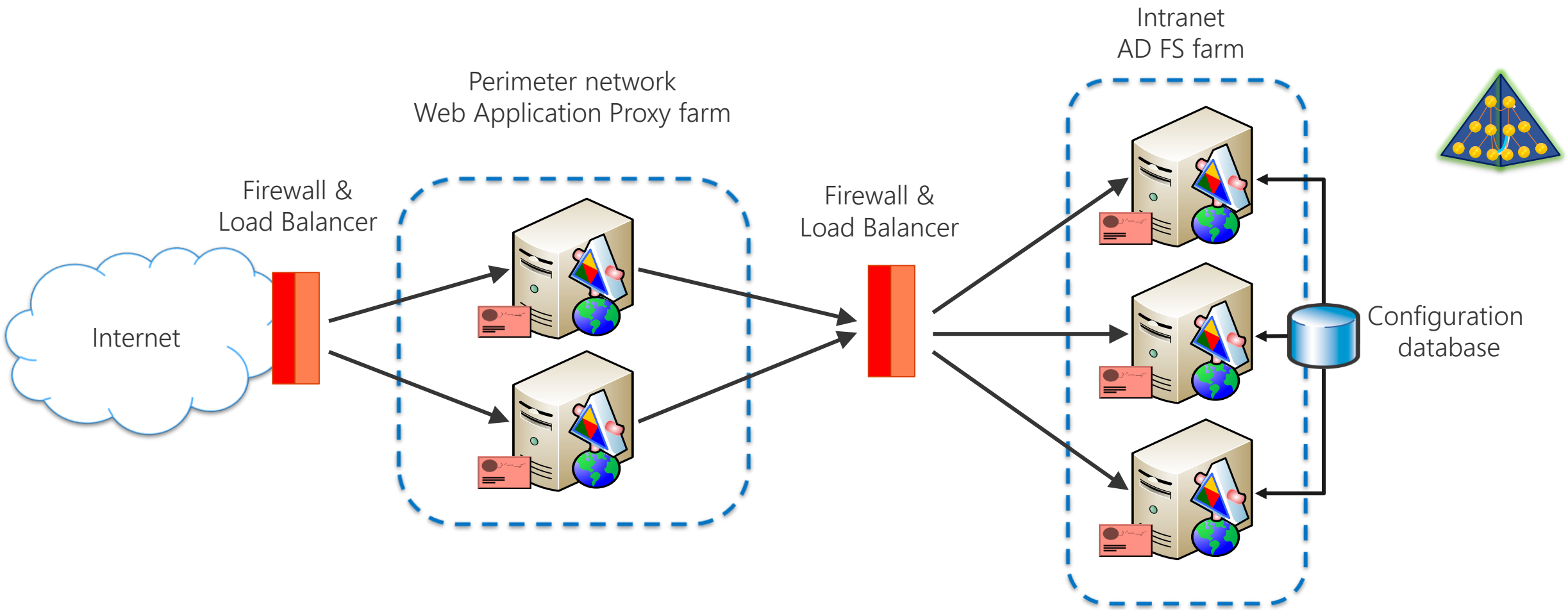
On-premises user sign-in to Azure AD



Federation


Directory Synchronization
Claims-aware app
Your AD FS
Your AD
App trusts Azure AD
Azure AD Trusts your AD FS
Browse app
Not authenticated
Redirect to your Azure AD
Home realm discovery – via UPN
Redirected to your AD FS
Authenticate
Return ST for consumption by Azure AD
ST
ST
Redirected to Azure AD
Process token
Return new ST
ST
ST
Send Token
Retrieve full user details if required
Return cookies and page

Federation at what cost?



No fully supported as a WAP replacement

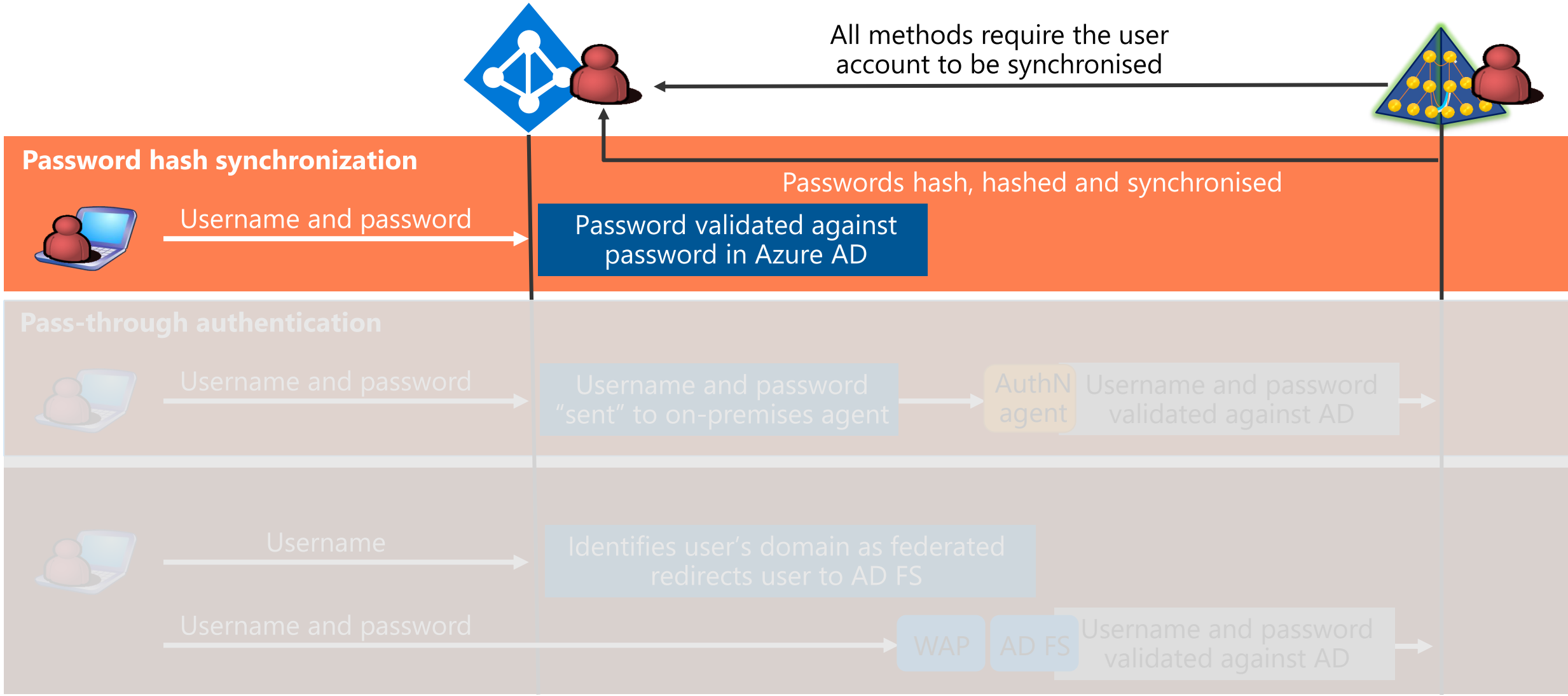
To federate or not? The facts…

- Federation gives you
  - SSO via on premises AD credentials
    - Seamlessly authenticate to AD FS when the client is attached to the corporate network
      - Now supported by Seamless SSO for PHS and PTA
  - Passwords remain on-premises
    - Now supported via PTA
  - On-premises authentication policies
    - Now supported via PTA
  - On-premises authentication methods (multi-factor)
  - Conditional access via AD FS
    - Capabilities++ provided by Azure AD
- Federation requires
  - On-premises AD FS infrastructure with high-availability
  - High-availability for the company's Internet connection
    - Remote workers will not be able to authenticate to Azure AD If the link is down
  - Planned recovery from the loss of AD FS availability

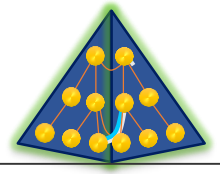
To federate or not? More facts…

- Federation may require manual certificate rollover
  - Auto renewal possible for most configurations (AD FS auto certificate rollover enabled)
- Federation **doesn't** give you
  - Cloud authentication scalability
  - Identity Protection
    - Requires P2 license
- PHS & PTA
  - Cloud authentication
  - Cloud scalability
  - Identity protect
- PTA
  - Simple deployment of agents
  - Automatic update of on-premises agents
  - Automatic rollover of certificates
  - Requires high-availability for the company's Internet connection

On-premises user sign-in to Azure AD

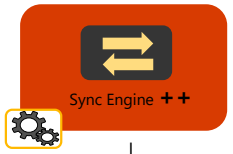


Password synchronization



MD4 hash of password stored in unicodePwd attribute

Azure AD Connect



Requests unicodePwd attribute values via MS-DRSR replication protocol

Encrypts MD4 with salt and MD5 hash of RPC session key

Sends result & salt

Decrypts to obtain MD4 hash of password

MD4 hash expanded, salt added input to PBKDF2 function 1000 interactions of HMAC-SHA256

Result sent to Azure AD

Password stored as original MD4 after processing with salt + PBKDF2 + HMAC-SHA256

Note: The on-premises Azure AD Connect AD account requires AD permissions:

Replicate Directory Changes
Replicate Directory Changes All

Sign in

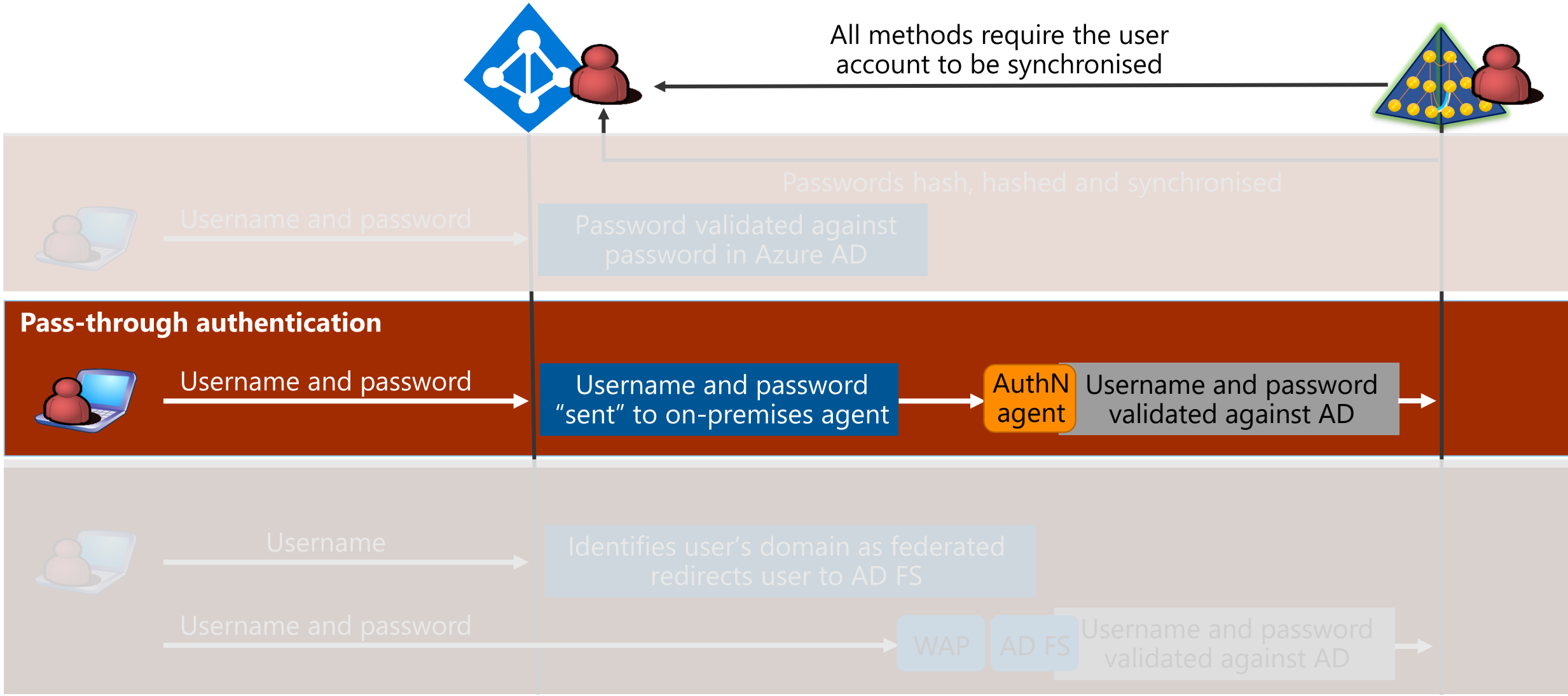
Does supplied password value, after processing with MD4, with salt, PBKDF2 and HMAC-SHA256, match stored value for user?

PBKDF = password based Key Derivation Function (RFC 2898)

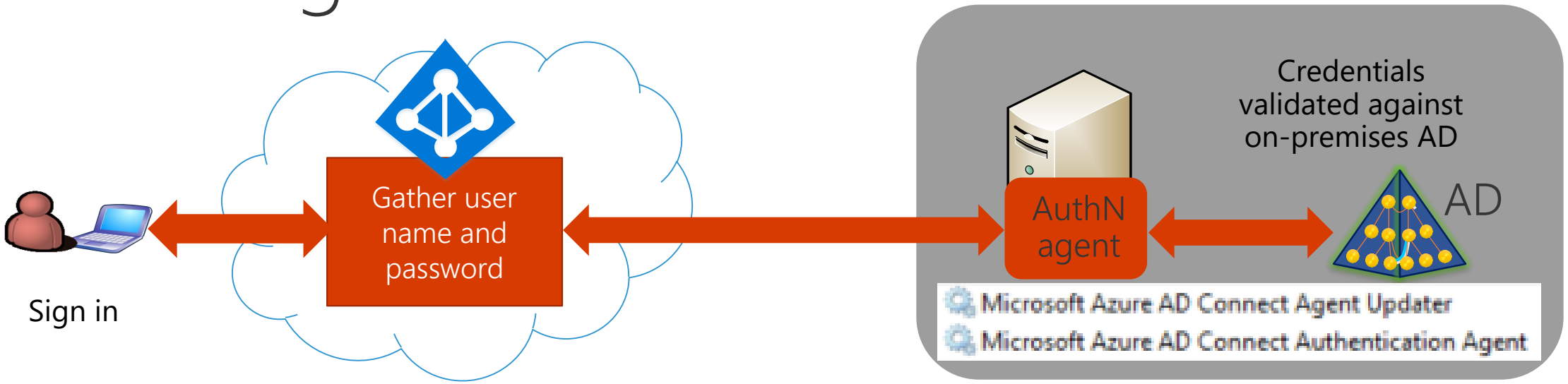
Password synchronization facts…

- On-premises password complexity applies to synchronized users
  - If an administrator changes the cloud password using PowerShell the Azure AD password policy applies
- An locked out on-premises AD account can still be active in the cloud
  - The cloud password for a PHS user is set to never expire
- A disabled on-premises AD account will not be reflected in Azure AD until the next sync cycle
  - Potentially 30 mins delay
- PHS can be used in addition to federation and used as a fall-back

On-premises user sign-in to Azure AD



Pass-through authentication

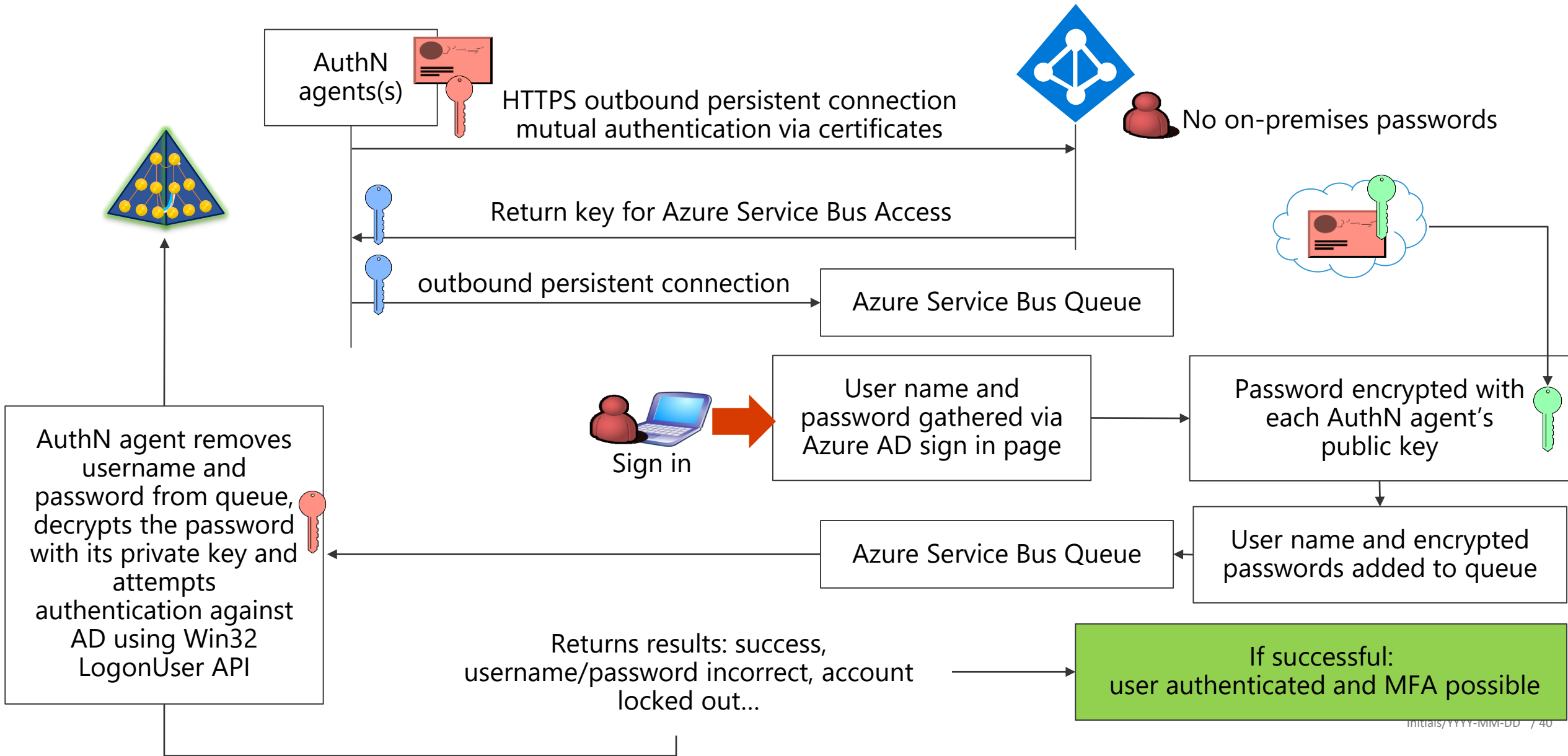


- The pass-through authentication agent (AuthN agent) only requires outbound firewall ports
  - Port 80 and 443
- Multiple agents can be deployed for fault tolerance and performance
  - Three agents should provide required performance
- All communications via mutually authenticated HTTPS

Pass-through authentication installation

- Each agent has its own unique certificate and private key
  - Azure AD periodically triggers the renewal of certificates and keys

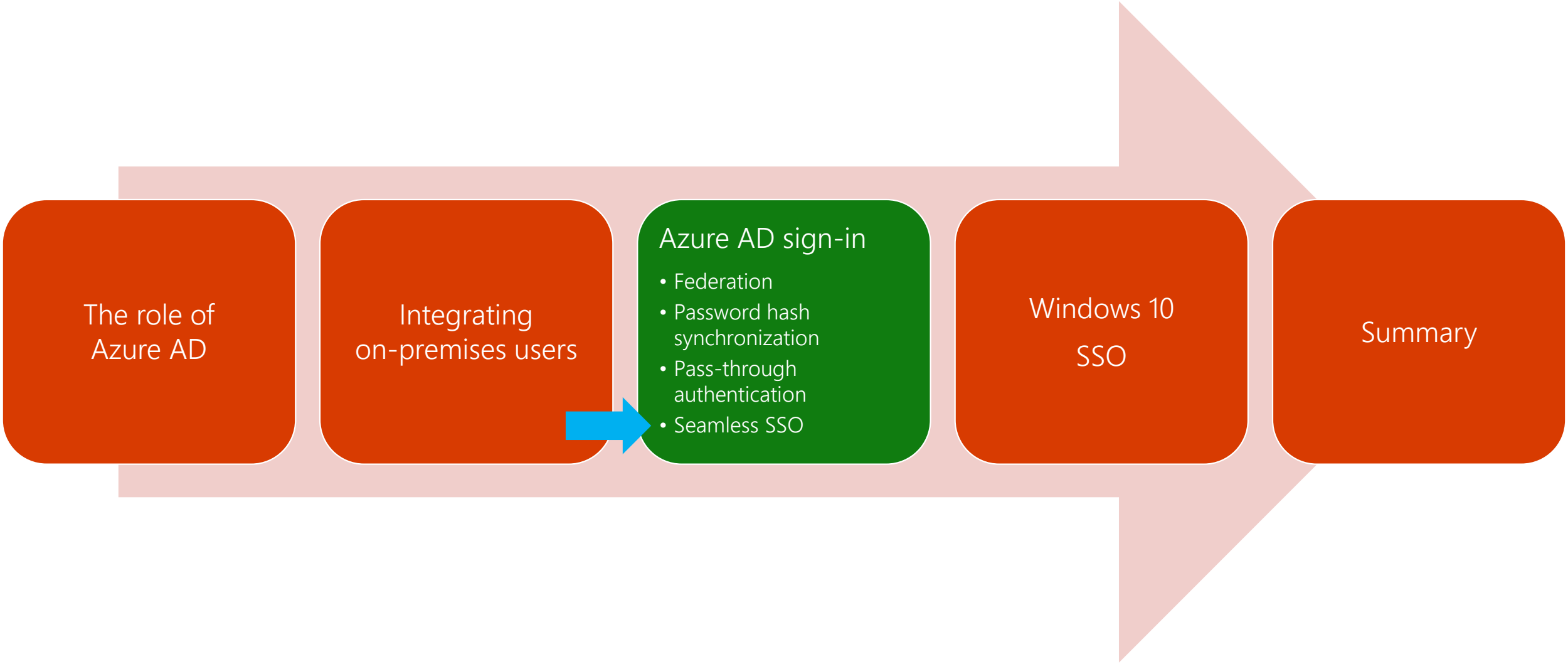
Pass-through authentication in action



Pass-through authentication the facts…

- No on premises passwords in the cloud
- All on-premises password policies operational
- Account lockout/disabled operational
- Does not support on-premises MFA
  - Azure AD MFA supported
- Works with Alternate ID
- Does not provide SSO for on-premises credentials
  - Requires Seamless SSO
- Requires high-availability for the company's Internet connection
  - Remote workers will not be able to authenticate to Azure AD If the link is down
- Currently does not support legacy auth
  - Example Office 2010

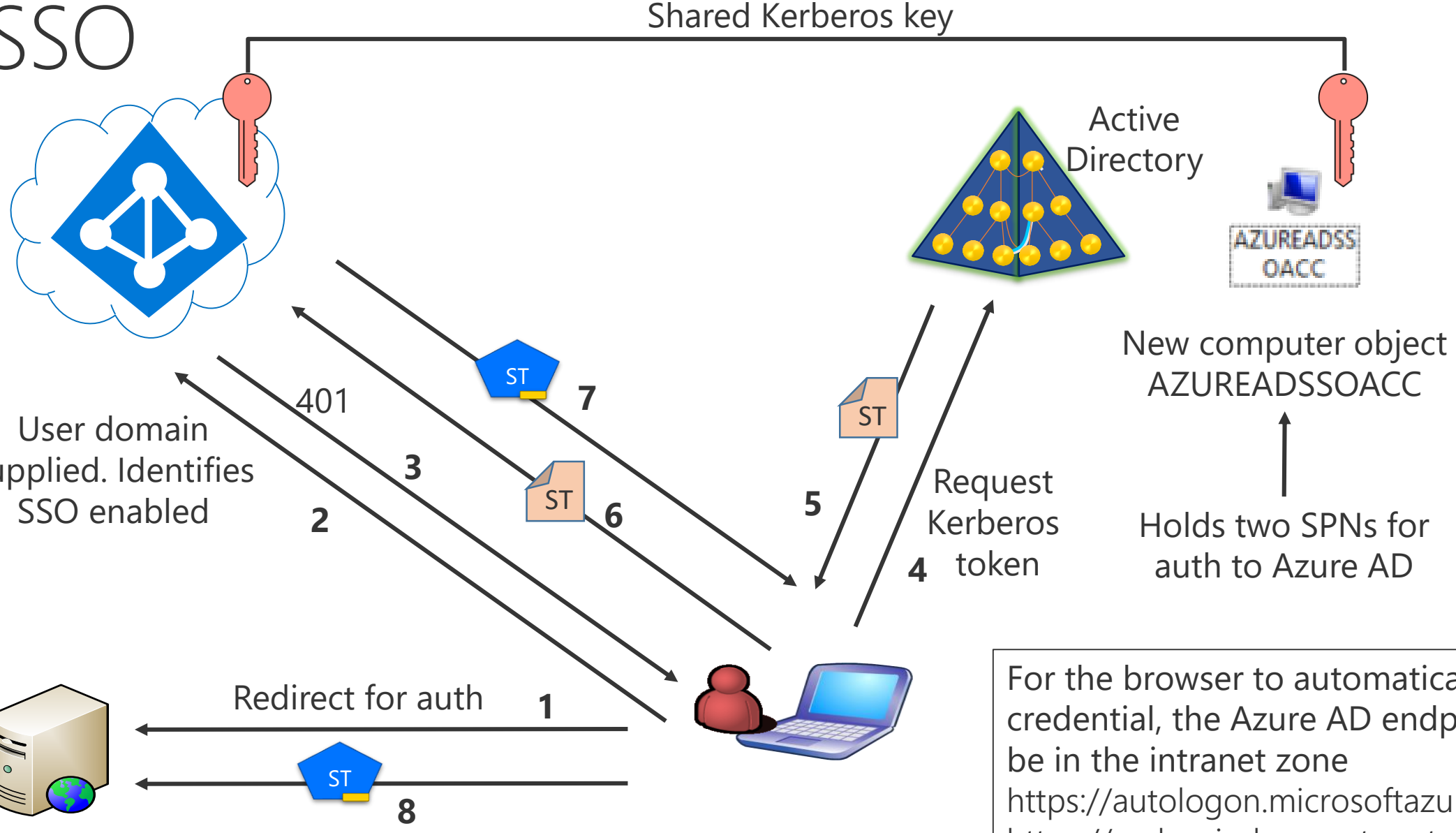
What's in this session



Seamless SSO, the facts…

- Works with pass-through authentication or password hash sync
- Users only need to type their name to authenticate to Azure AD
  - It is possible for applications to pass a domain_hint for seamless SSO
  - Supports Windows 7 and above
    - Windows 10 Edge not currently supported
  - Machine must be domain joined and have access to a DC
    - On corporate network or via remote access technology
  - Authenticates to Azure AD with a Kerberos token
  - Available with all versions of Azure AD
  - Supports Alternate ID
  - Support for multiple browsers and OSs
    - Including Safari and Mac

sSSO



For the browser to automatically pass the credential, the Azure AD endpoints must be in the intranet zone
https://autologon.microsoftazuread-sso.com
https://aadg.windows.net.nsatc.net

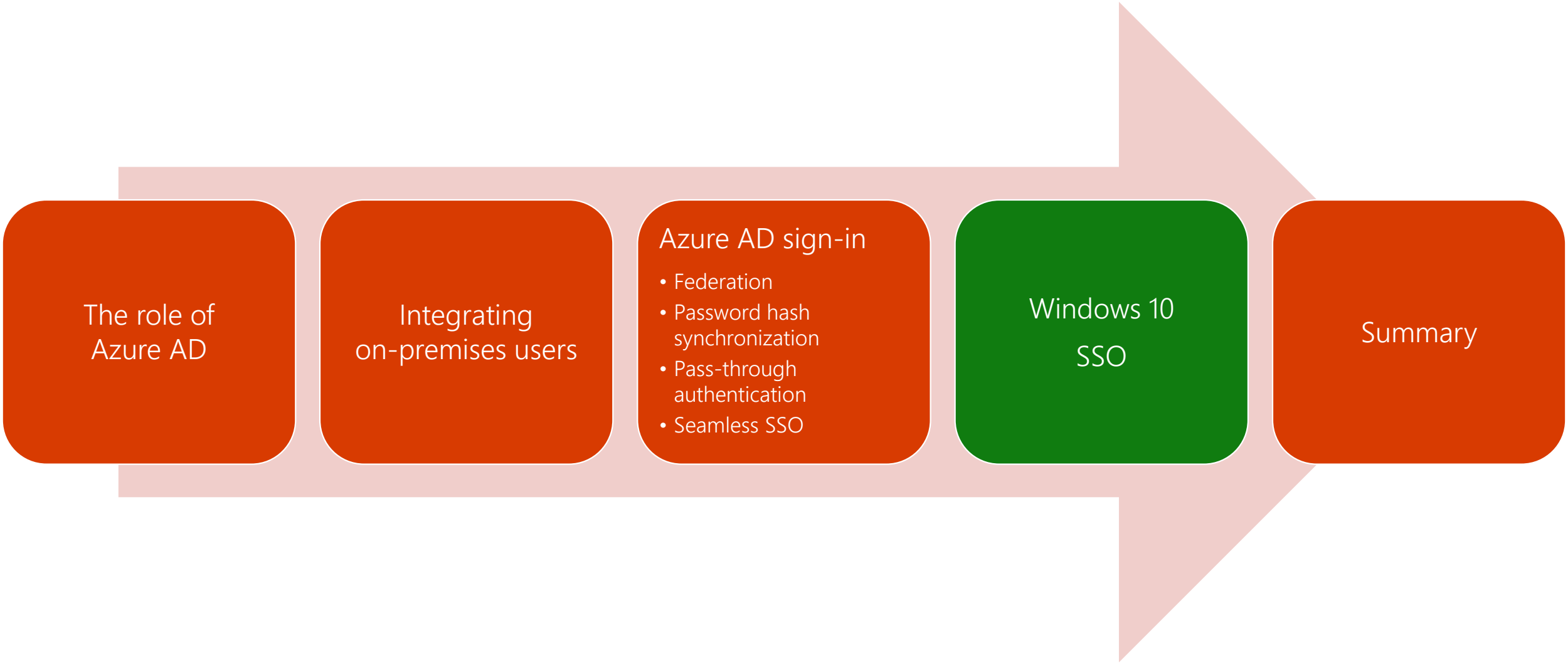
Kerberos authentication

- Seamless SSO can be configured with PTA or PHS
- If the user is connected to the corporate AD domain and sSSO succeeds, the authentication to Azure AD is Kerberos
- If the user is not connected to the corporate AD domain, authentication will fall-back to select authentication method (PTA or PHS)
- If an incompatible or mis-configured browser is detected, authentication will fall-back to select authentication method (PTA or PHS)

Kerberos Key

- The security of your on-premises authentication relies on the integrity of the Kerberos key
  - Recommended to roll the key every 30 days
- For details of managing key rolling see:
  - https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-faq
- Automatic key rollover is on the roadmap!

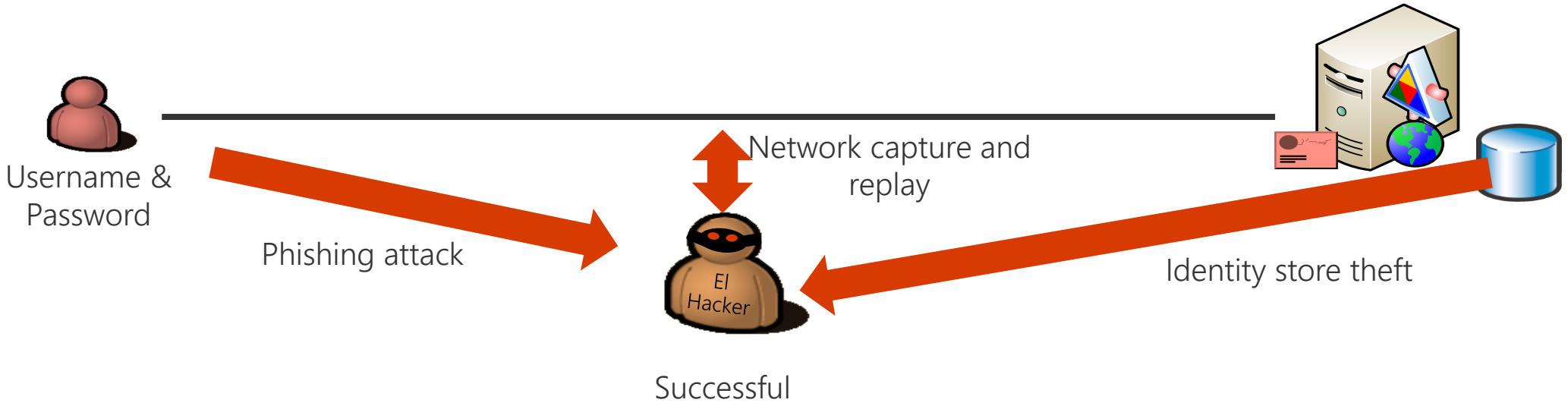
What's in this session



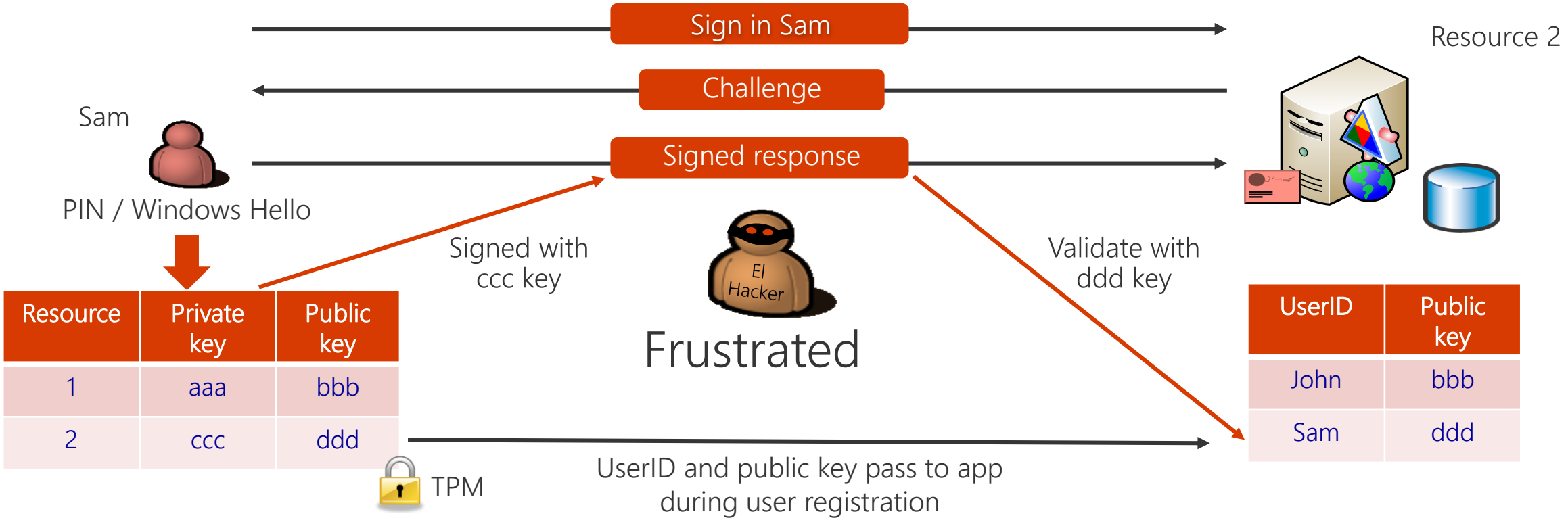
Windows 10 and AD users

- Hybrid Azure AD Join
  - AD Domain Join with automatic Azure AD registration
  - All the benefits of Group Policy / SCCM / Intune
- When users sign-in to their device they get a
  - Kerberos token for on-premises AD and Primary Refresh Token (PRT) for Azure AD access
- Single sign on to all Azure AD authenticated resources
  - No requirement to have access to a DC
- Conditional access policies can be based on the users device
- Windows Hello for Business can be used for authentication

Passwords are dangerous



Microsoft Hello for Business (simplified)



- Hello sign in for Azure AD and AD/AD FS 2016
- Part of FIDO Alliance standard

FIDO = Fast ID Online

Azure AD B2C: "IDMaaS for Applications"

The goal of Azure AD B2C is to provide all IDM functions an app needs to handle a customer audience – preview coming soon

- Azure AD security, availability, and scalability for customer IDM
- Adds B2C features to Azure AD
  - Social IdPs and "application local accounts"
  - Self-service sign up, password reset, profile management
  - Customizable sign in and sign up UI
  - Same protocols, libraries, and programming model
- Consumption based pricing
  - Meters for # of users and # of authentications

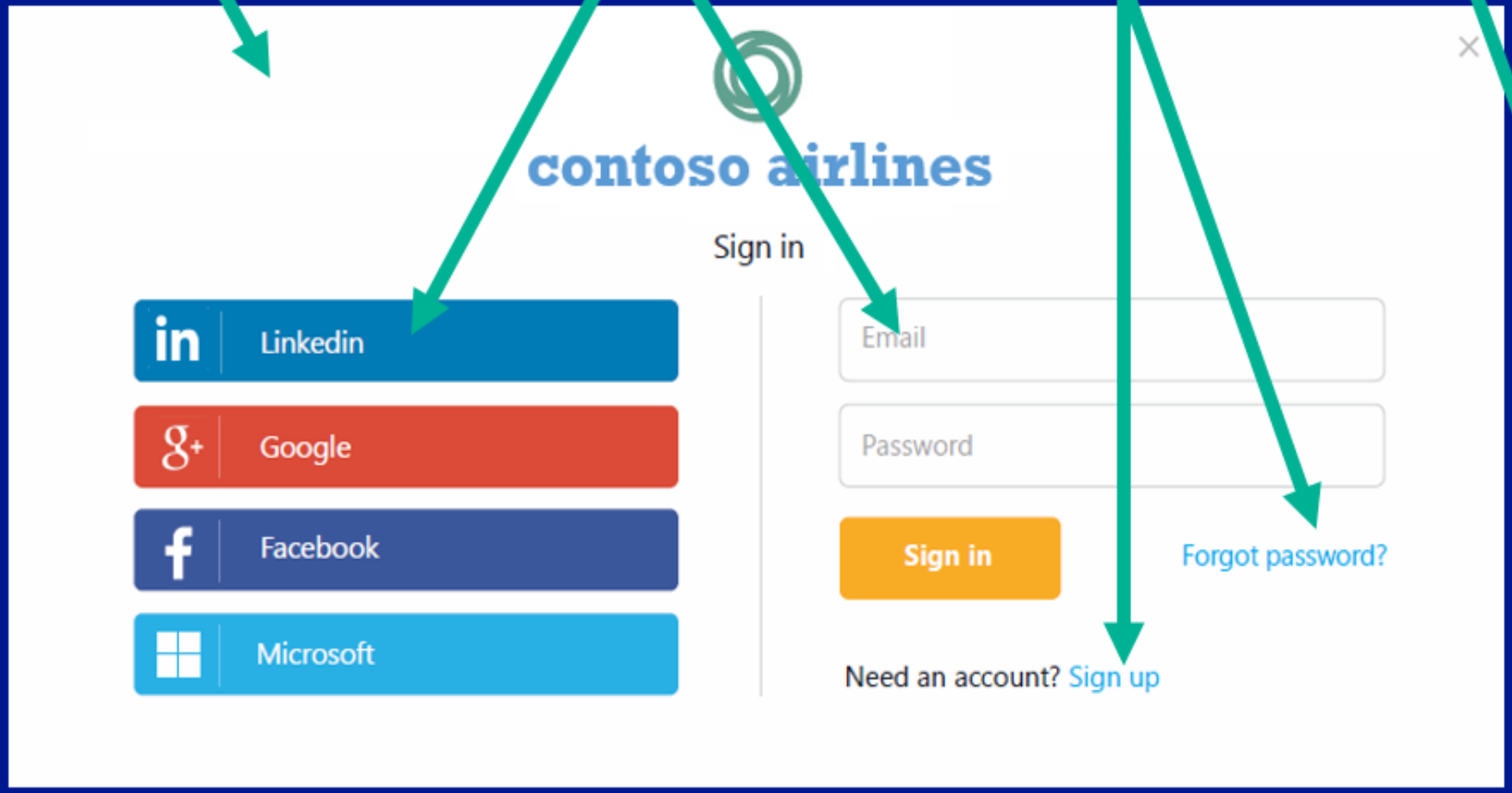
Azure AD B2C

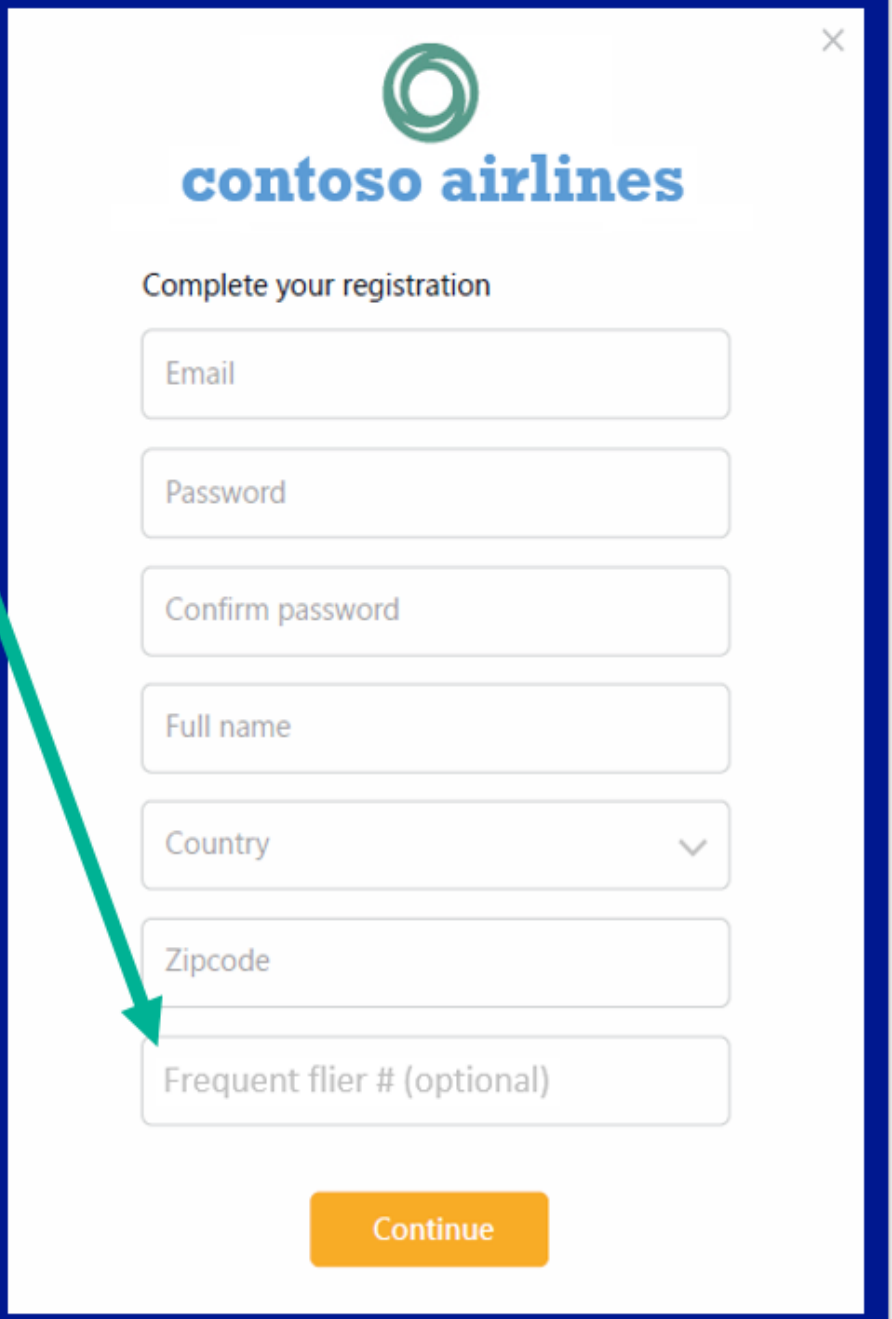
Customize UI

Social and local accounts

Handles sign up, password reset

Define attributes to gather during sign up



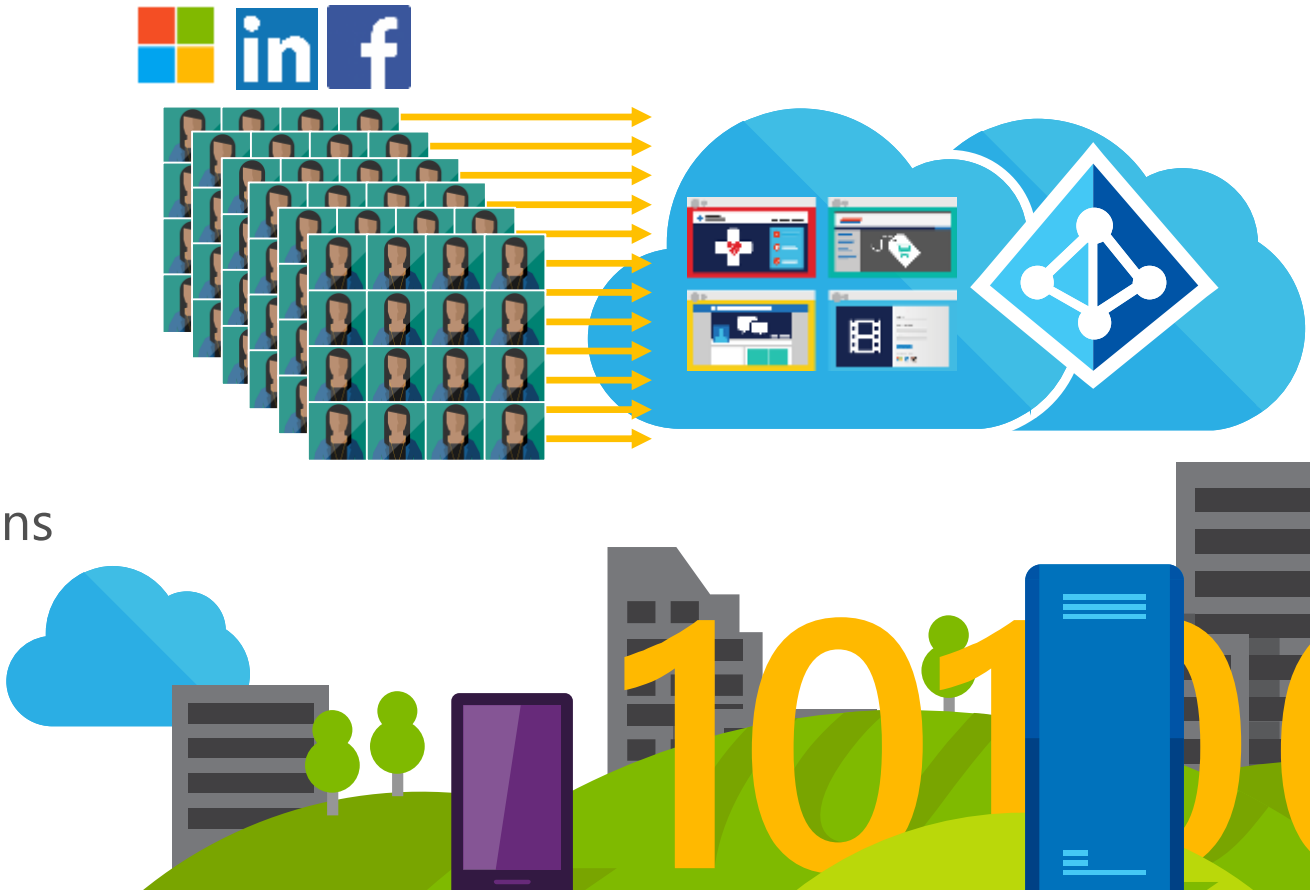


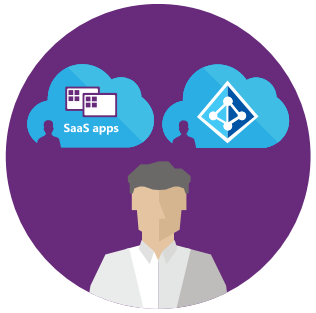
Azure Active Directory B2C

Consumer identity and access management in the cloud

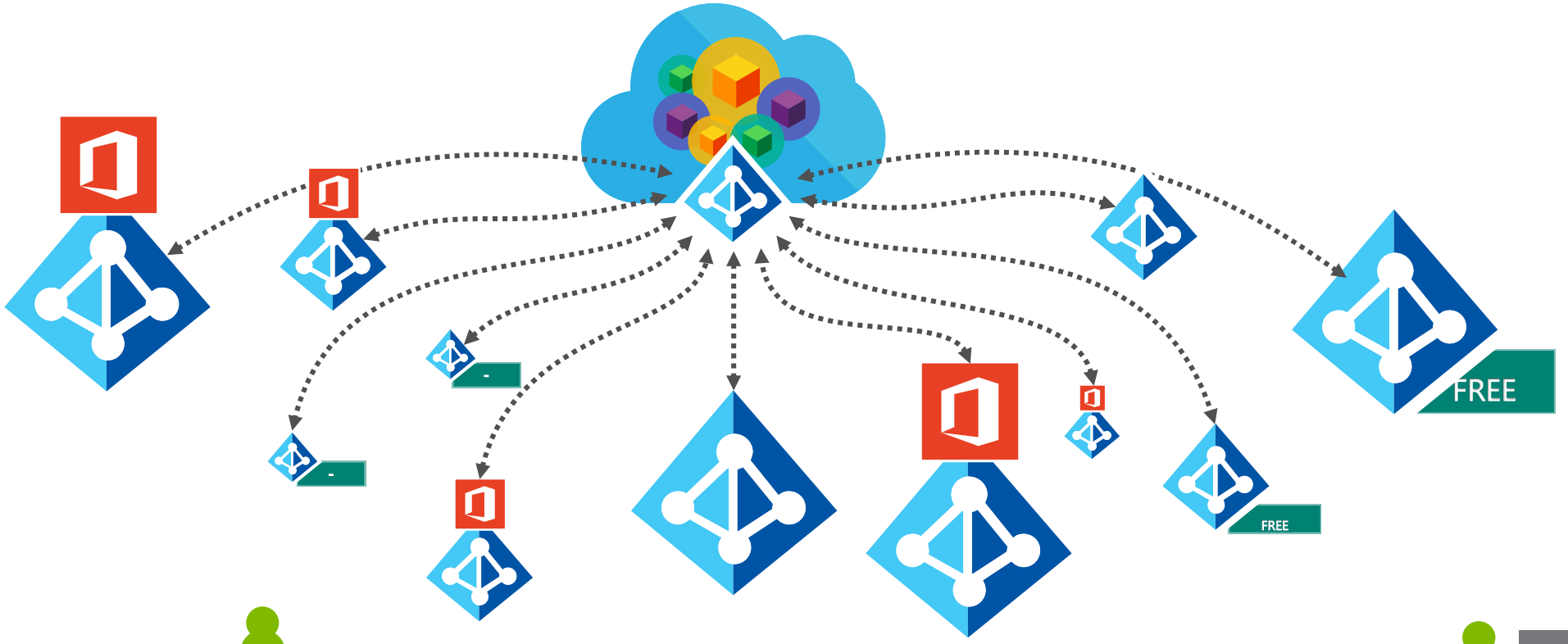
A highly available, global, cost-effective identity management service for consumer-facing applications

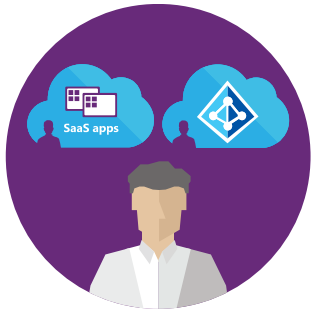
- Improve connection with your consumers
- Pay only for what you use
- Scale to hundreds of millions of consumers
- Help protect your consumers' identities
- Let consumers use their social media accounts
- Customizable workflows for consumer interactions



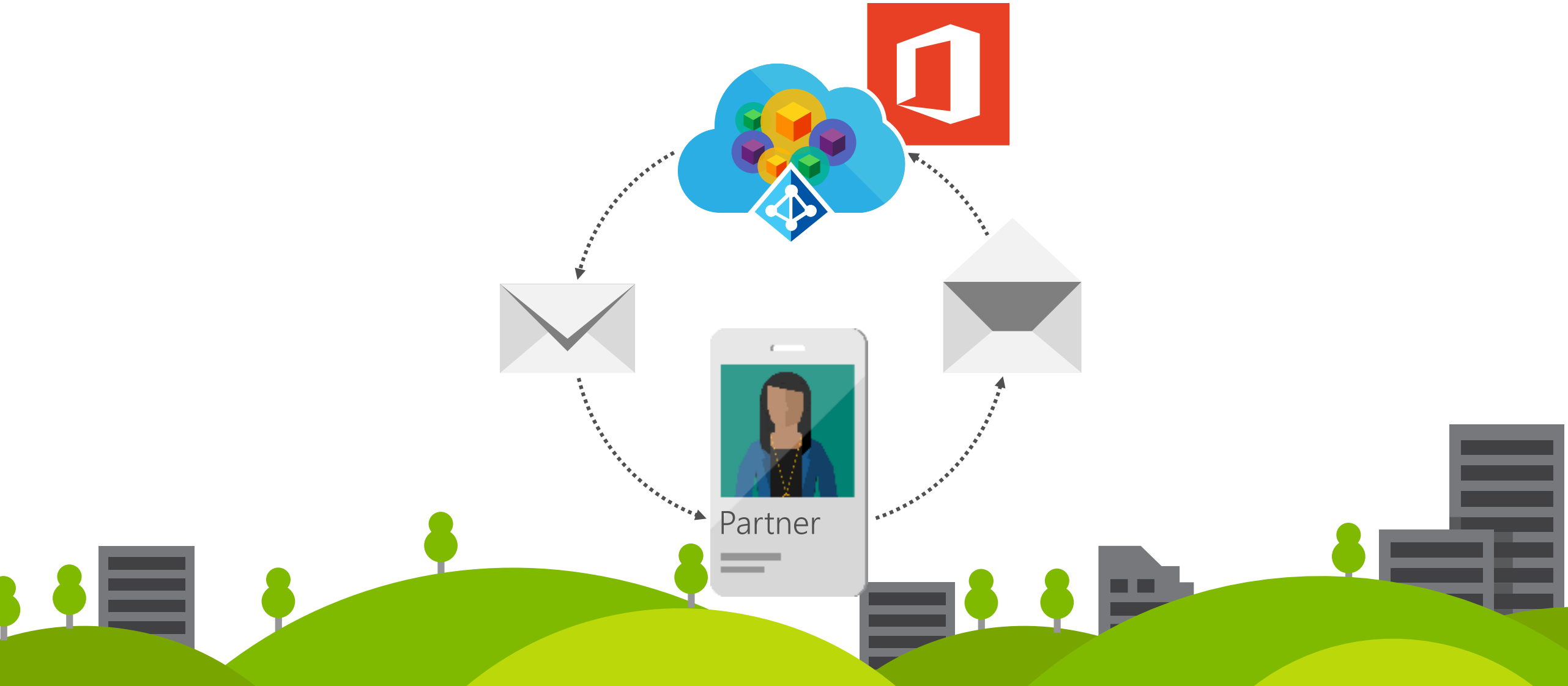


"I need to let my partners access my company's apps using their own credentials."





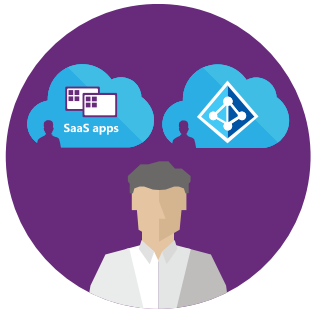
B2B collaboration – Email verified provisioning



Your employees need to collaborate with partners: Easily share data and applications with the right people in the right companies
Your Partners want simplicity No new accounts to manage, No federation to configure, No servers to install
Admins want security Control and oversight, Granular auditing and monitoring of partner access,World class security and protection

B2B collaboration

Securing identities beyond your own employees and expanding to your network of partners and contractors is critical to protecting your company data. Azure Active Directory B2B collaboration as additional functionality available in all Azure AD editions, provides simplified management and security for partner and other external user access to your in-house resources using Azure AD as the control plane. This includes access to popular cloud applications such as Salesforce, Dropbox, Workday, and of course Office 365, in addition to mobile, cloud, and on-premises claims-aware applications.
B2B collaboration improves security, as partners manage their own accounts and enterprises can apply security policies to partner identities access.
Azure Active Directory B2B collaboration is easy to configure with simplified signup for partners of all sizes even if they don’t have their own Azure AD via an email-verified process. It is also easy to maintain with no external directories or per partner federation configurations.
Make your Azure Active Directory the center of your cross-organization collaboration.
Azure Active Directory B2B collaboration will be provided at no additional cost with all Azure AD editions.
Partners receive email created by Azure AD B2B collaboration feature. If his organization has an Azure Active Directory tenant (Office 365, EMS, Intune, Azure , Azure AD Premium or Basic) he can directly access the resource his invited for .
If the partner organization doesn’t have an Azure AD directory then by accepting the invitation from the email a free Azure AD directory is created for him



Achieve simple and secure partner access

Partners manage their own credentials

Partners use their own creds to access your org.

Users lose access when they leave the partner org.

No external directories.

No per partner federation.

Organizations manage access

You control partner access in your directory:

- app assignment
- group membership
- custom attributes

Partners of all sizes

Thousands of bulk invites at a time.

Partners with Azure AD sign in to accept invite.

Other partners simply sign up to accept invite.

What is Azure Multi-Factor Authentication?

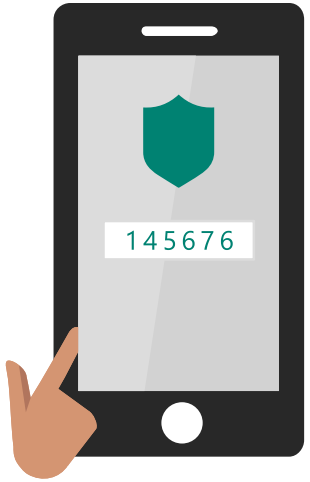
A st Identity and Access
ma lso included in
remium

ccess to both on-
pplications by
ditional level of

Trusted by thousands of enterprises to authenticate employee, customer, and partner access.

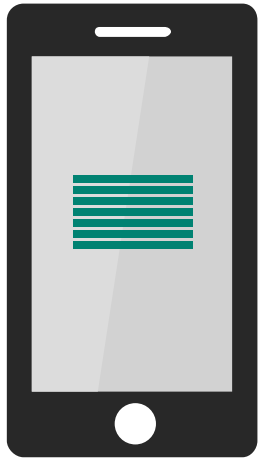
How it works

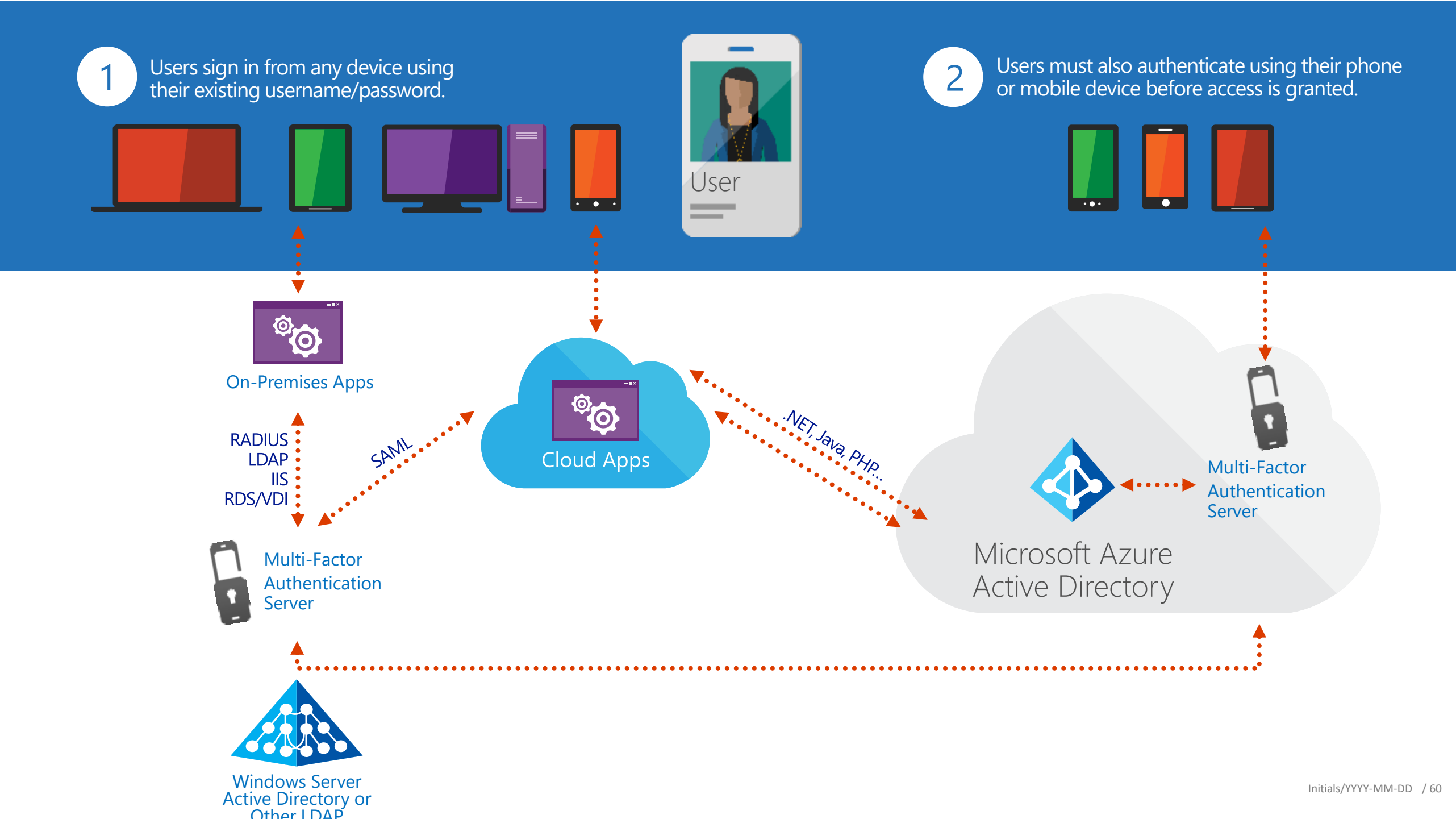
Mobile apps



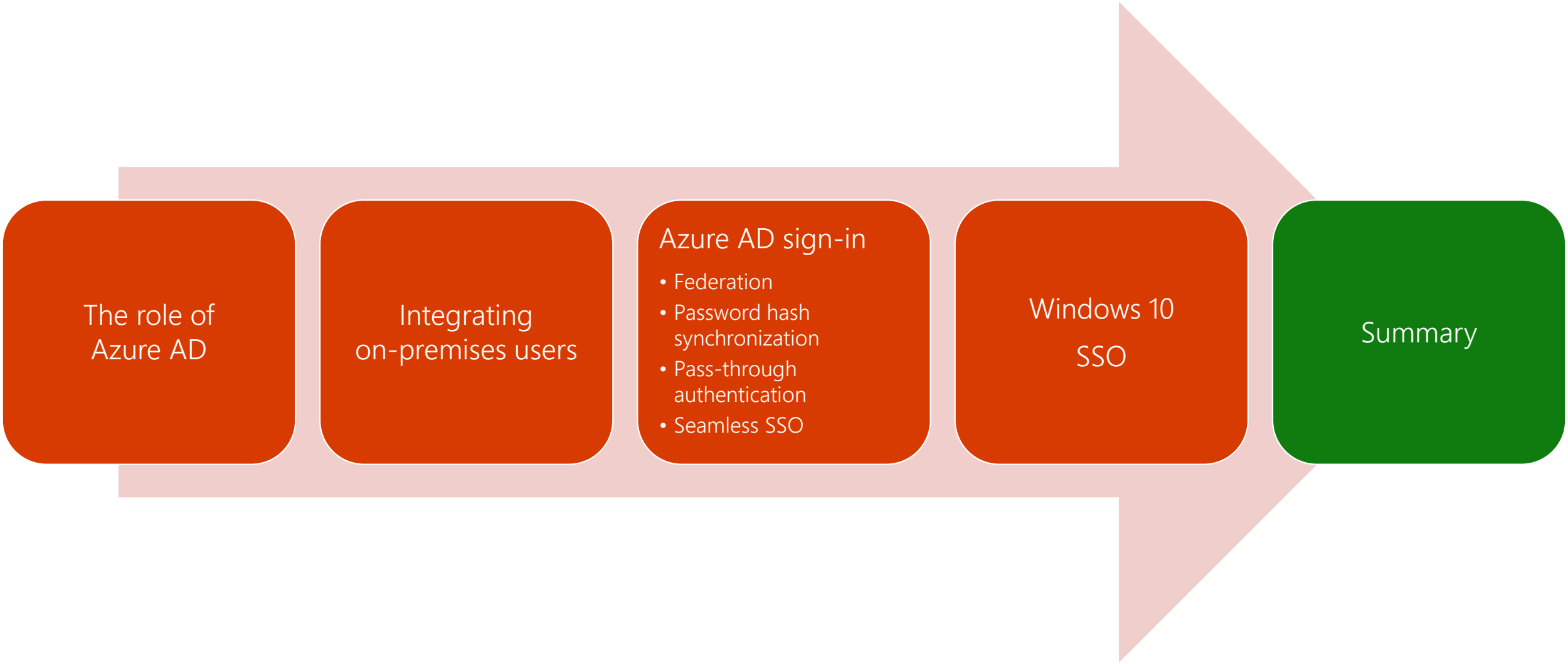
Phone calls

Text messages




1
Users sign in from any device using their existing username/password.
User
2
Users must also authenticate using their phone or mobile device before access is granted.
On-Premises Apps
RADIUS
LDAP
IIS
RDS/VDI
SAML
Cloud Apps
.NET, Java, PHP...
Multi-Factor Authentication Server
Microsoft Azure Active Directory
Multi-Factor Authentication Server
Windows Server Active Directory or Other LDAP

What's in this session



Feature summary	PTA + sSSO	PHS + sSSO	ADFS
Authentication against credentials held on-premises	Yes	No	Yes
Single-Sign-On	Yes	Yes	Yes
Passwords remain on premises	Yes	Salted hash synced	Yes
On-premises MFA solution	No	No	Yes
Azure AD MFA	Yes	Yes	Yes
On-premises password policies	Yes	Partial	Yes
On-premises account enable/disable	Yes	Delayed (30 mins)	Yes
On-premises password lockout	Yes	No	Yes
Conditional access	Yes++	Yes++	Yes
Credentials captured from user via Azure AD UI	Yes	Yes	No
Protection against on-premise account lockout	Smart Lockout	N/A	Extranet Lockout
Cost of implementation	Medium	Low	High
Scalability/fault tolerance	Cloud scalability	Cloud scalability	Complex
AuthN fails for remote workers if the on-premises Internet connection is down. Requires HA solution.	Yes	No	Yes
On-going maintenance for authentication	Automated	None	SSL certificate management
Azure AD Connect Health monitoring	Not integrated	Limited	Yes
Azure AD Identity Protection (requires P2 license)	Yes	Yes	No

Recommendations

- New customers:
  - Use cloud authentication (PTA or PHS)
    - Leverage conditional access and Azure AD MFA
  - Existing customers with AD FS
    - Keep AD FS for authentication if it meets all your requirements
    - If using AD FS for authentication to apps, switch to Azure AD for authentication to apps
- Enable Seamless SSO if your using PTA or PHS
  - Simple to deploy
  - Immediately enhances the sign-in experience for your users
  - Implement domain_hint for custom apps