

BUS5001 – Cloud Platforms and Analytics



IT TURNS OUT THAT THE
PEOPLE'S BIGGEST FEAR
ABOUT CLOUD COMPUTING ISN'T
'DATA SECURITY', IT'S 'WHAT
HAPPENS IF THERE'S A
THUNDERSTORM?'



© D.Fletcher for CloudTweaks.com

Week 04 – Security & Governance

Centre for Data Analytics and Cognition
La Trobe University, Australia

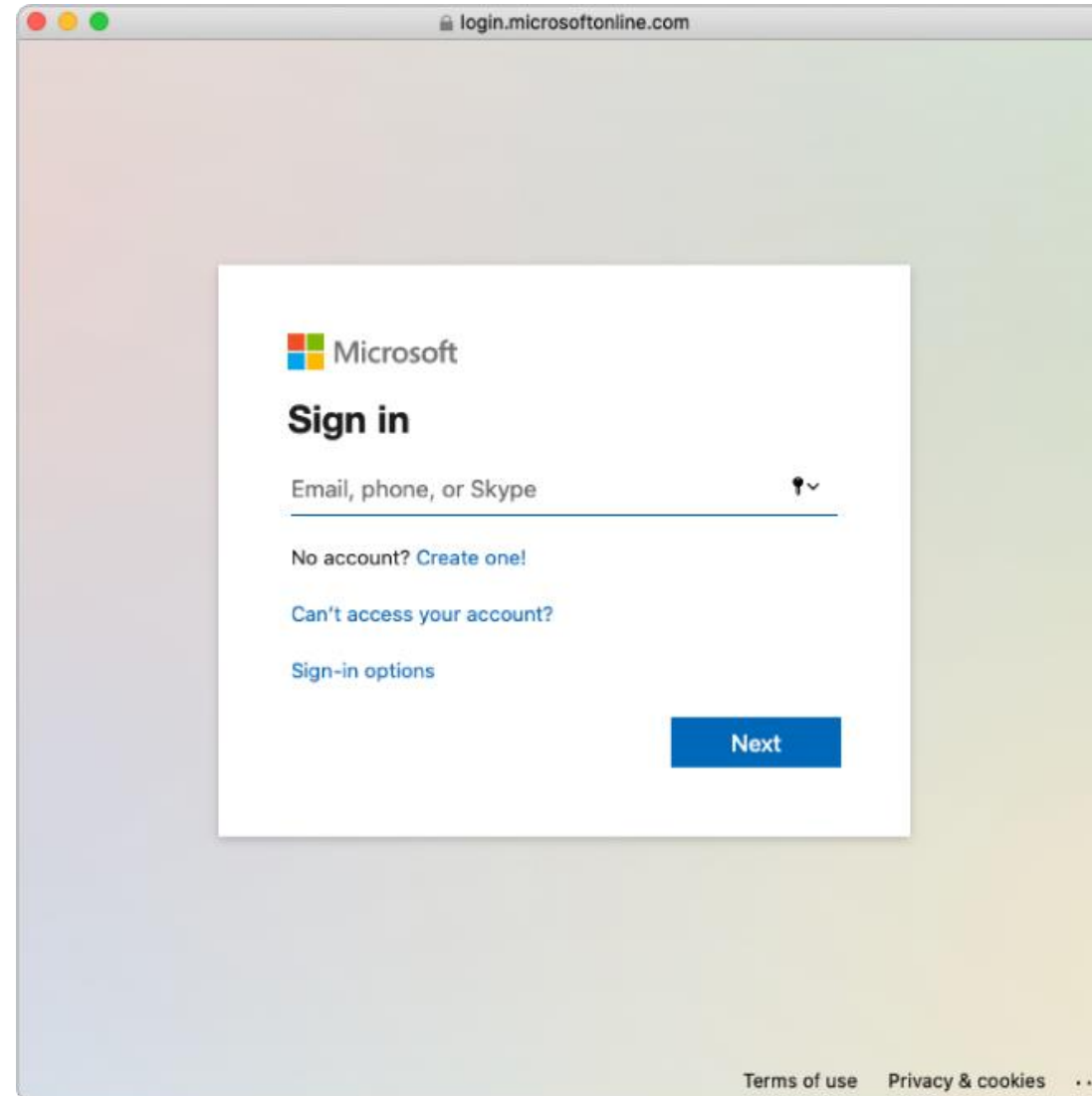
Different Perspectives of Security

- Data
- Application
- Compute
- Network
 - Perimeter
- Identity
- Physical

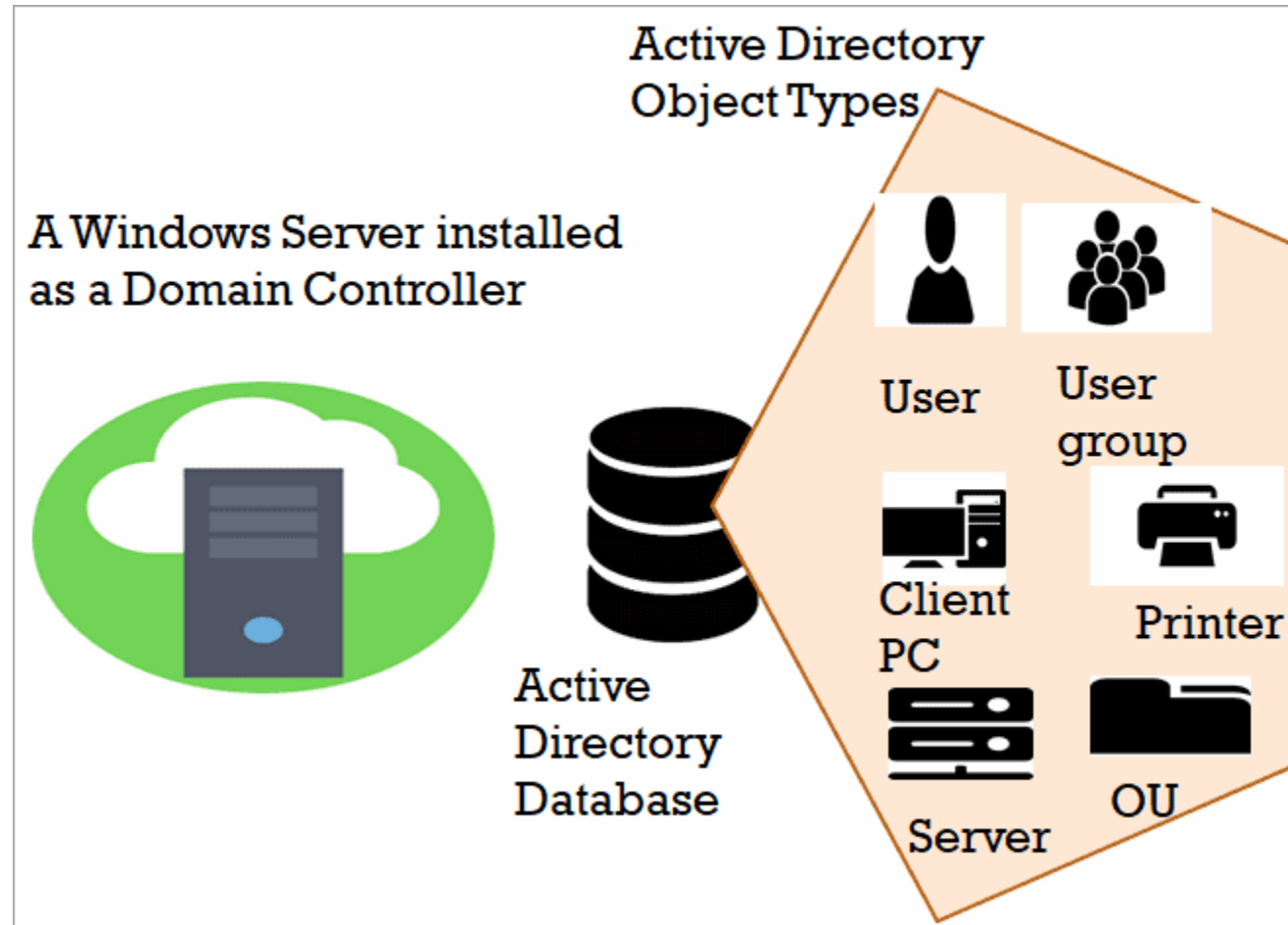
Authentication

- Determines who you are;
 - “Do we know you?”
 - “Are you who you say you are”?
- Ways to authenticate:
 - Passwords
 - Multi-Factor Authentication (MFA) – Additional evidence
 - Biometrics – Fingerprints or face recognition
 - Security Tokens – Special security devices

A Familiar Authentication Prompt



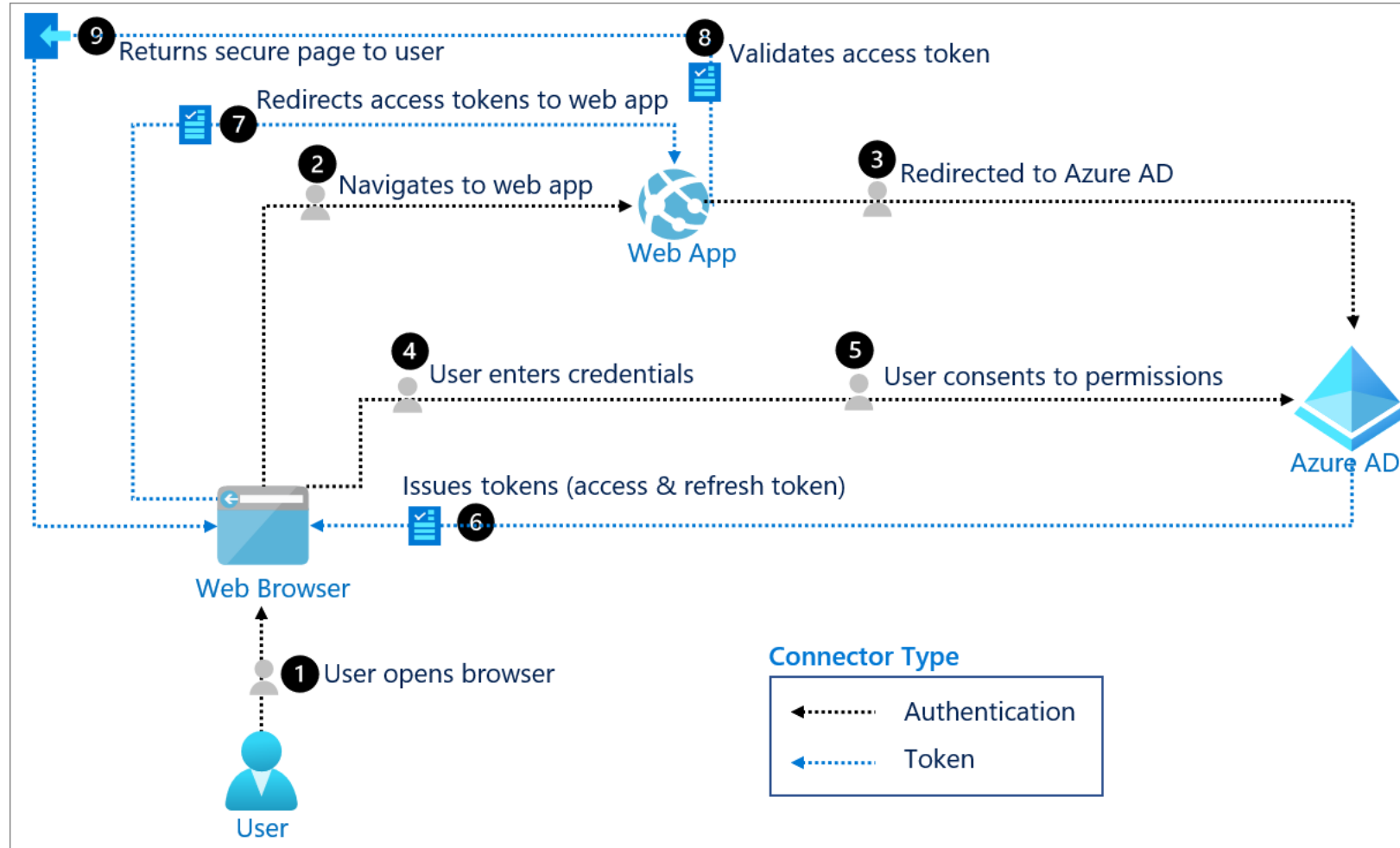
Active Directory



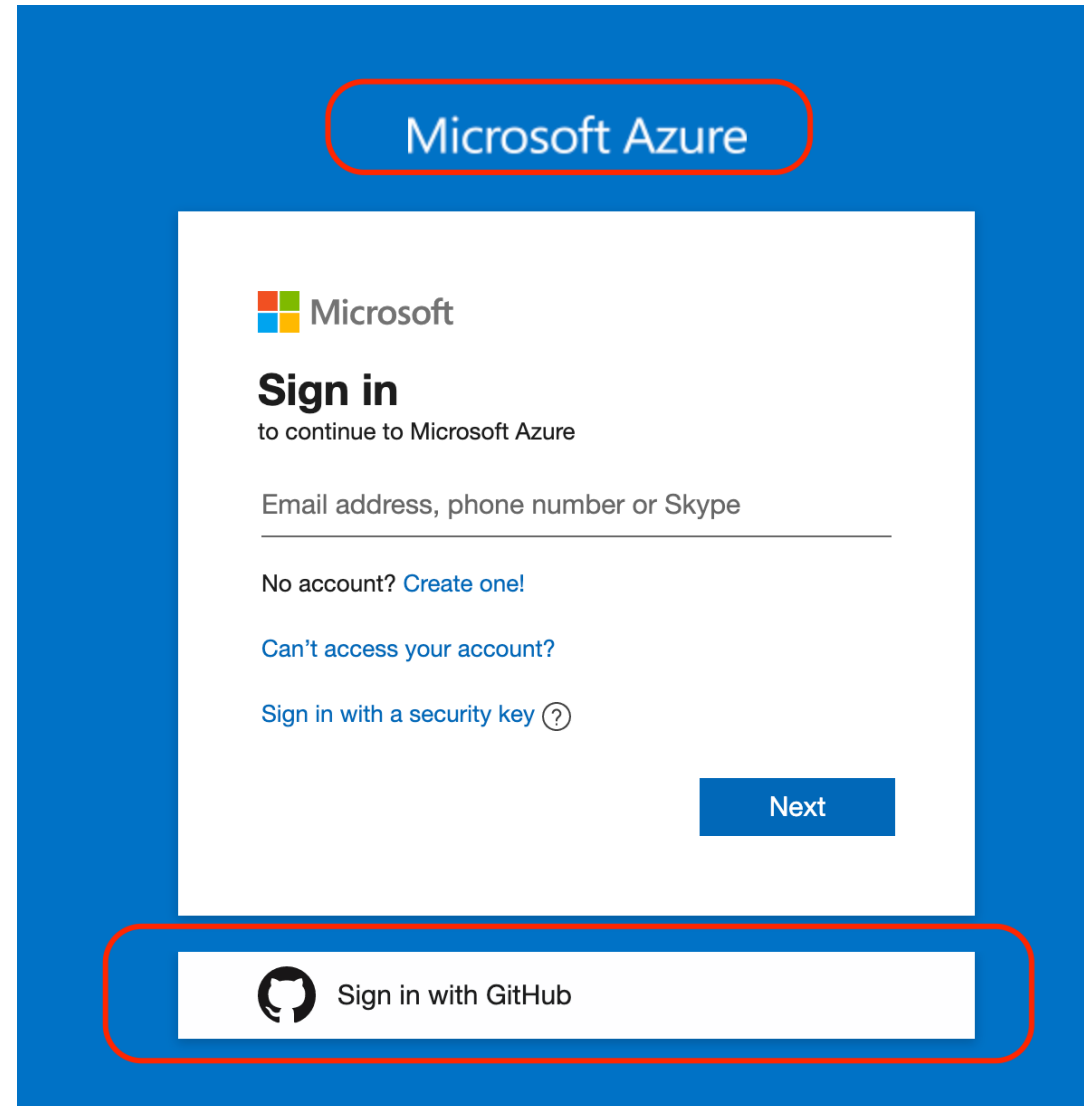
What does it do?

- Centralized Control: Manage users, computers, and devices from one location.
- Authentication & Authorization: Verifies user identities and controls access to resources.
- Organizational Structure:
 - Domains: Like different towns or cities, each with its own rules.
 - OUs: Smaller groups within domains to organize resources.
 - Forests & Trees: Connects multiple domains under one structure.
- Group Policy: Sets laws (security and configuration settings) across the network.
- Global Catalogue: A listing with information on all resources.
- Trust Relationships: Alliances between domains for resource sharing.

Authentication Process: OpenID Connect with Azure AD




Using a different Identity Provider



The image shows a screenshot of the Microsoft Azure sign-in interface. At the top, a blue rounded rectangle contains the text "Microsoft Azure". Below this, the Microsoft logo is followed by the text "Sign in to continue to Microsoft Azure". A text input field is labeled "Email address, phone number or Skype". Below the input field are three links: "No account? Create one!", "Can't access your account?", and "Sign in with a security key ?". A blue "Next" button is positioned to the right of the input field. At the bottom, a white rounded rectangle contains the GitHub logo and the text "Sign in with GitHub". Red rounded rectangles highlight the "Microsoft Azure" header and the "Sign in with GitHub" option.

Microsoft Azure

 Microsoft

Sign in
to continue to Microsoft Azure


Email address, phone number or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Sign in with a security key ?](#)

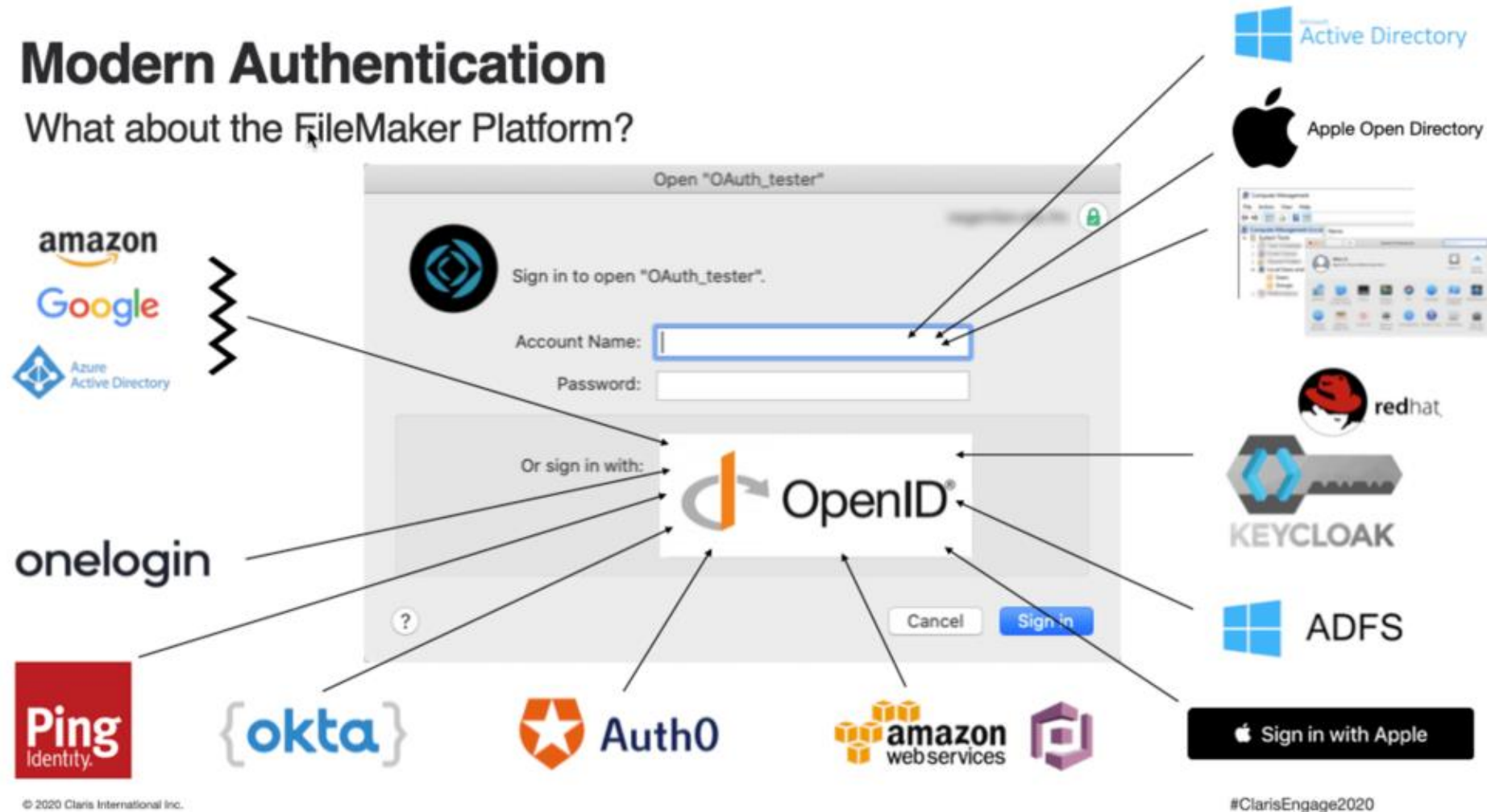
Next

 Sign in with GitHub

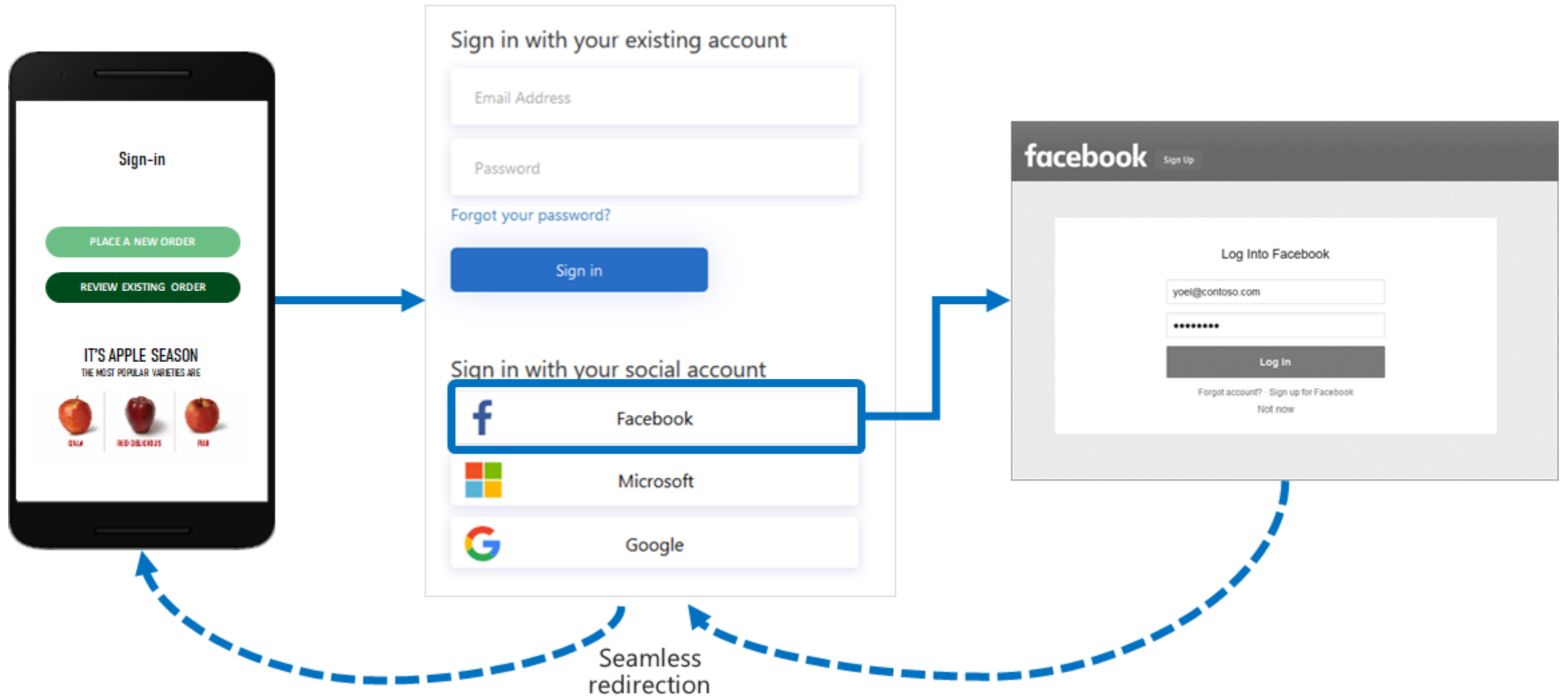
Identity Providers

Modern Authentication

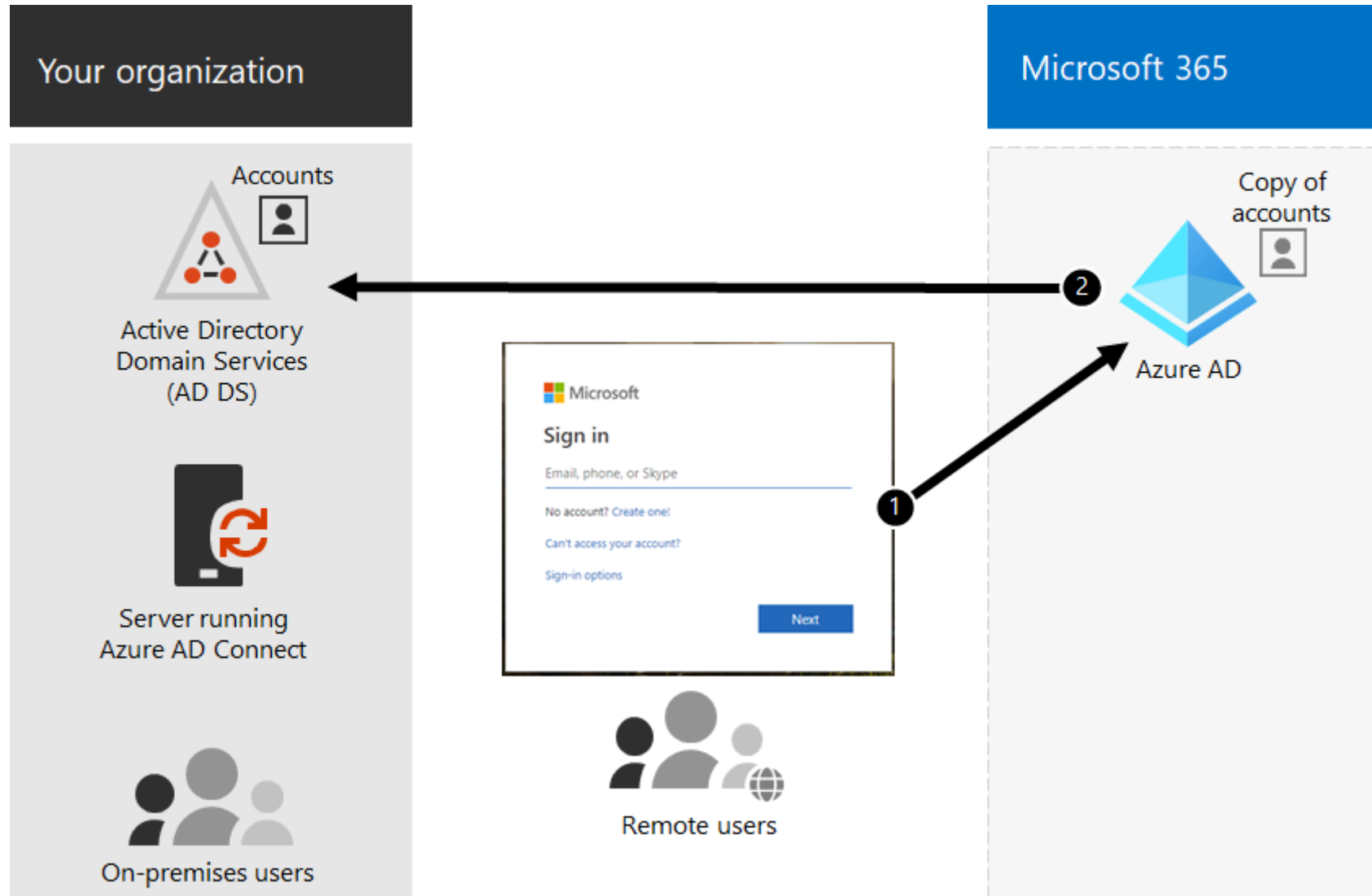
What about the FileMaker Platform?



Identity Providers



Single Sign On

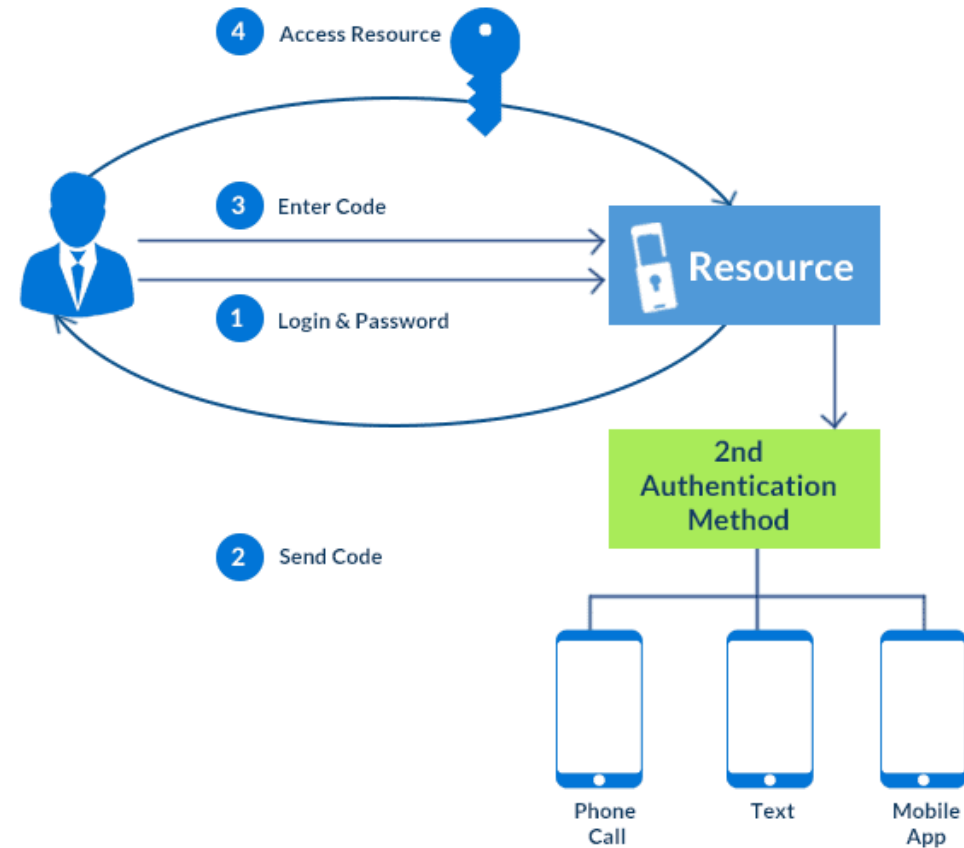


Multi Factor Authentication

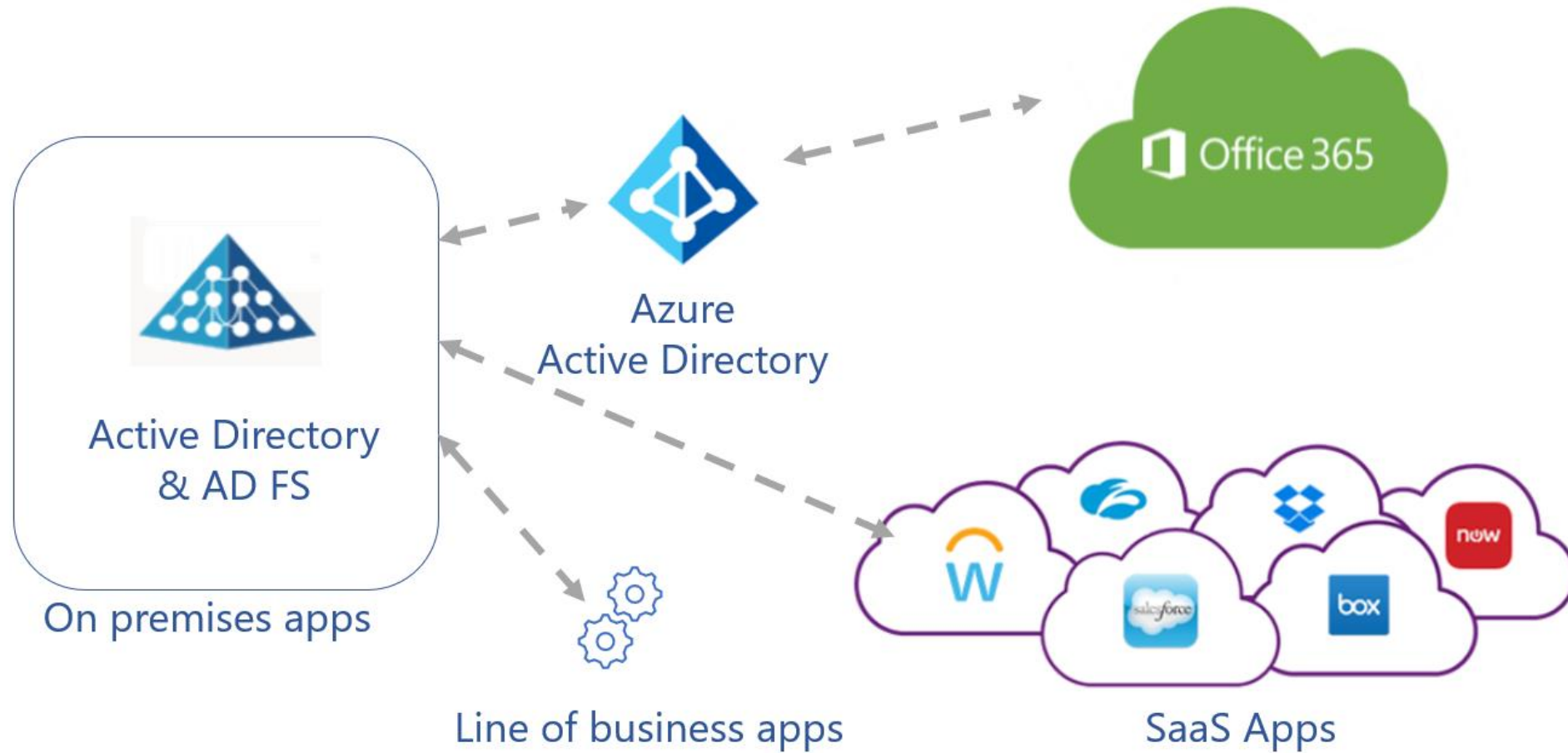
- More than one factor, e.g. 100 point identity for bank account
- Types
 - Knowledge – Something you know
 - Possession – Something you have
 - Physical – Something you are
 - Location – Where you are

Multi Factor Authentication

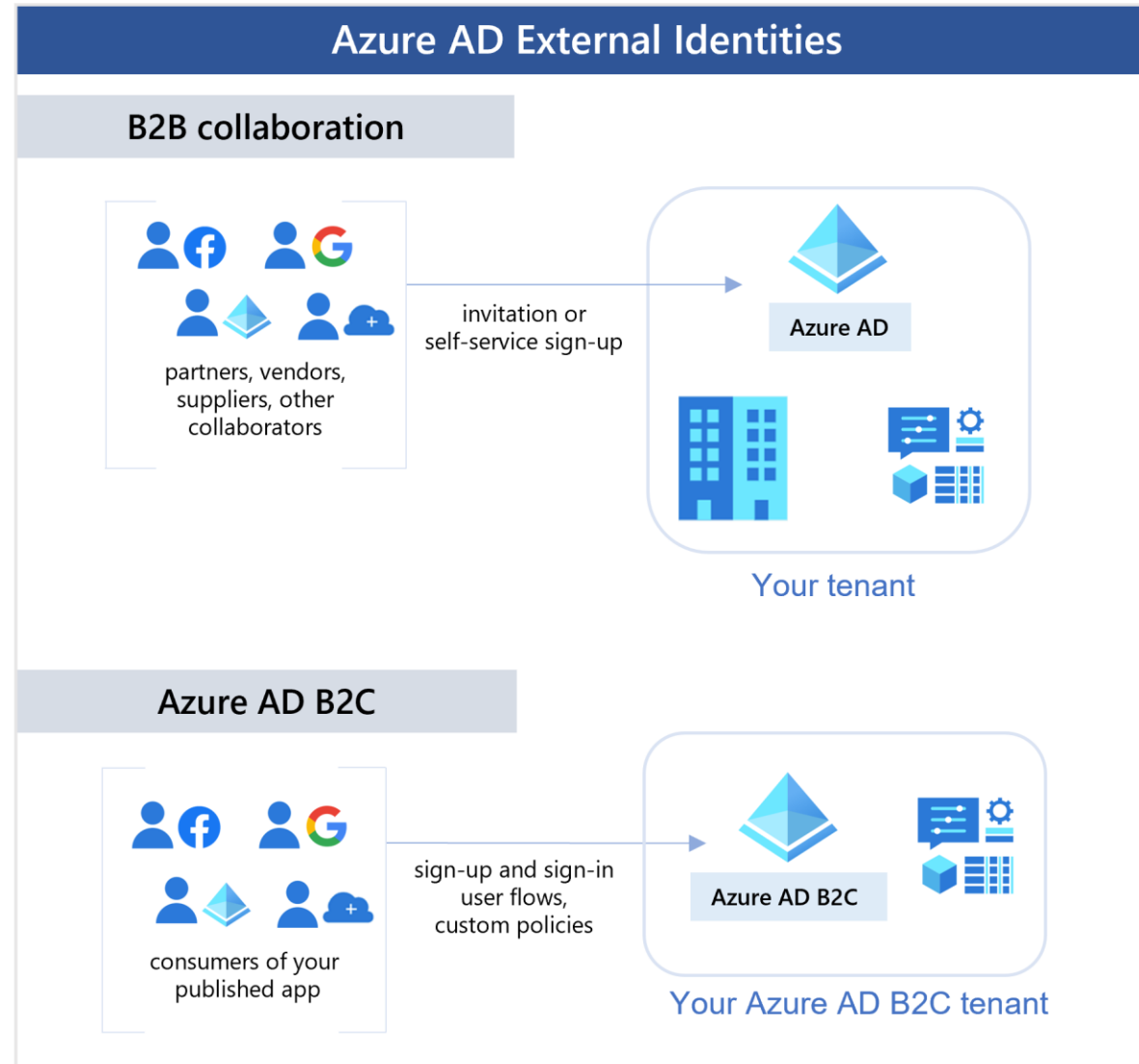
Multi Factor Authentication



Azure Active Directory



Azure AD B2B / B2C



Authentication – Personal Best Practices

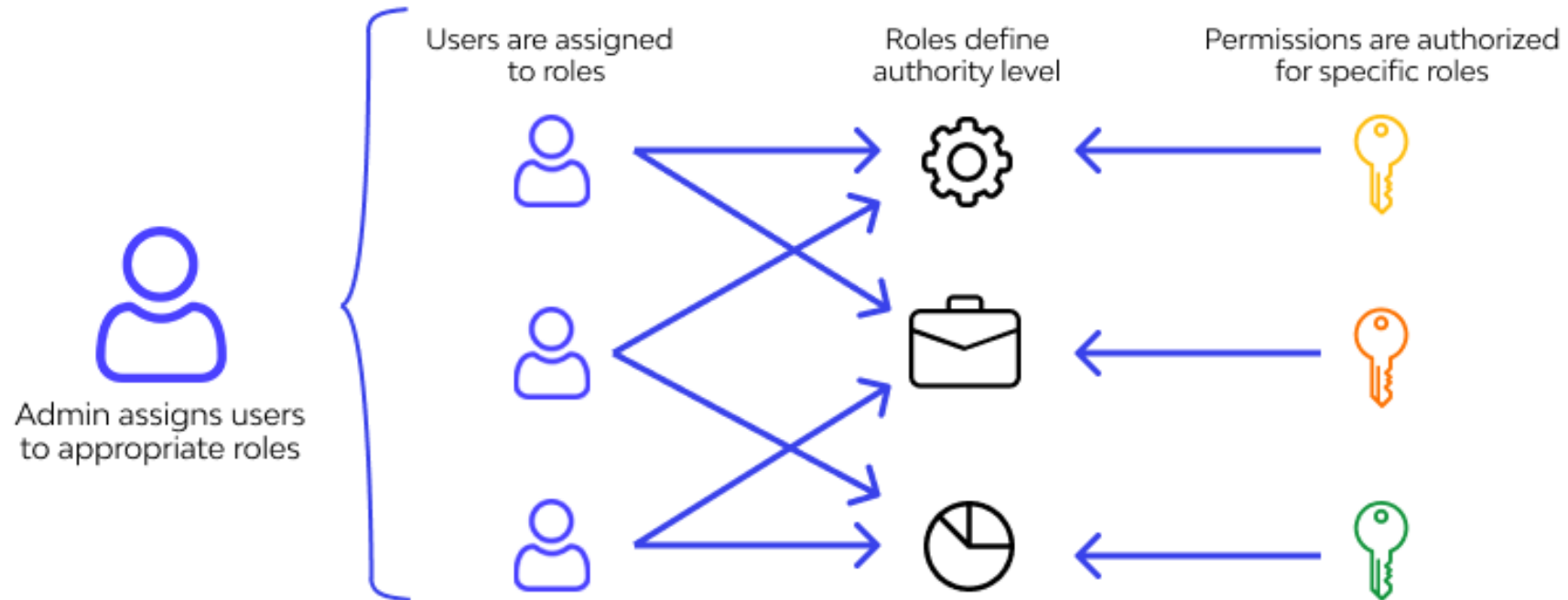
- Long complex passwords
- Password manager
 - <https://1password.com/password-generator/>
 - <https://www.random.org/passwords/?mode=advanced>
- Audit – <https://haveibeenpwned.com/>

Authorisation

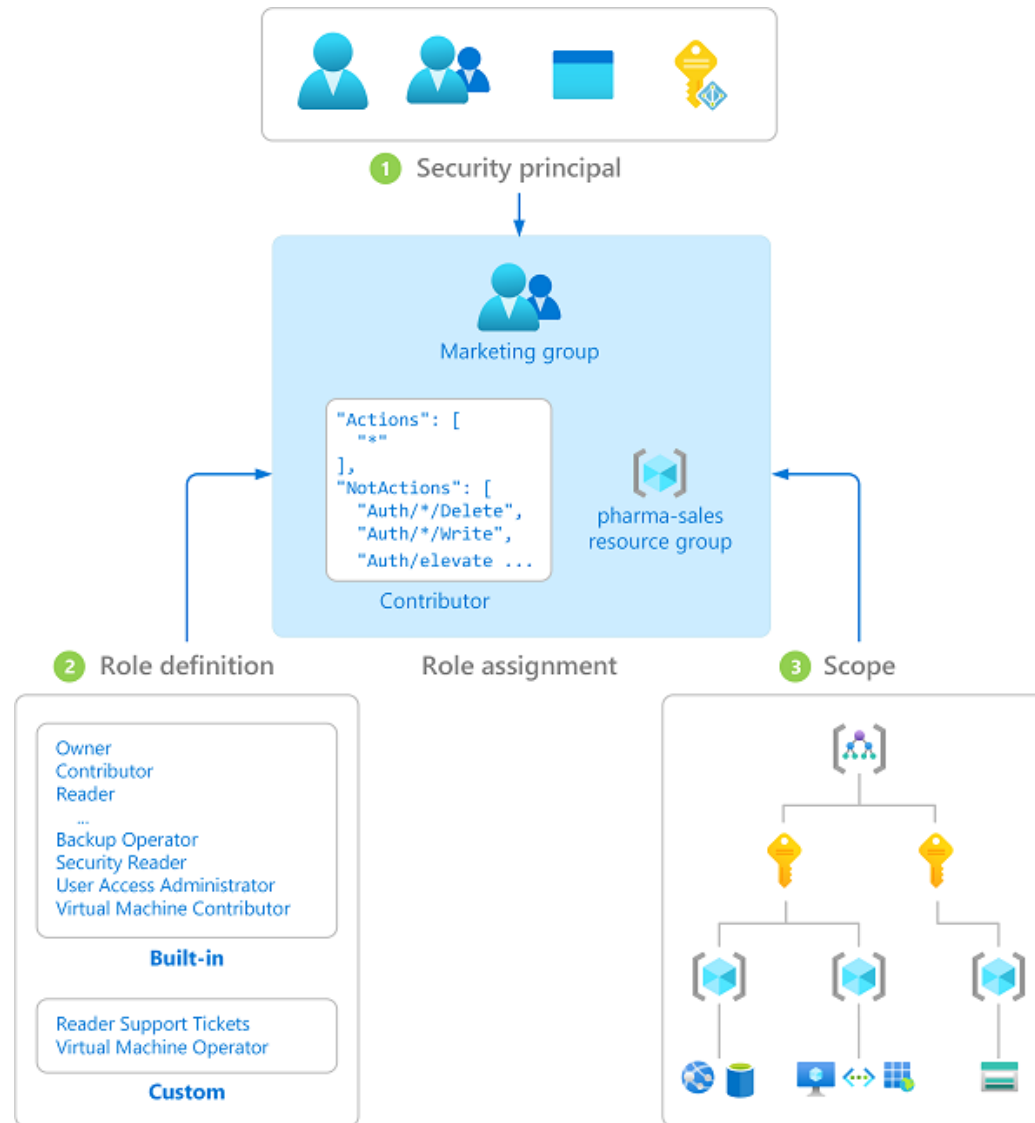
- Determine what you can do;
 - “Now that you have access what are the actions you can perform”?

RBAC (Role Based Access Control)

Role-Based Access Control



RBAC (Role Based Access Control)



Data Governance

- Data governance is a principled approach to managing data during its life cycle, from acquisition to use to disposal
- Data governance is everything you do to ensure data is secure, private, accurate, available, and usable. It includes the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle.



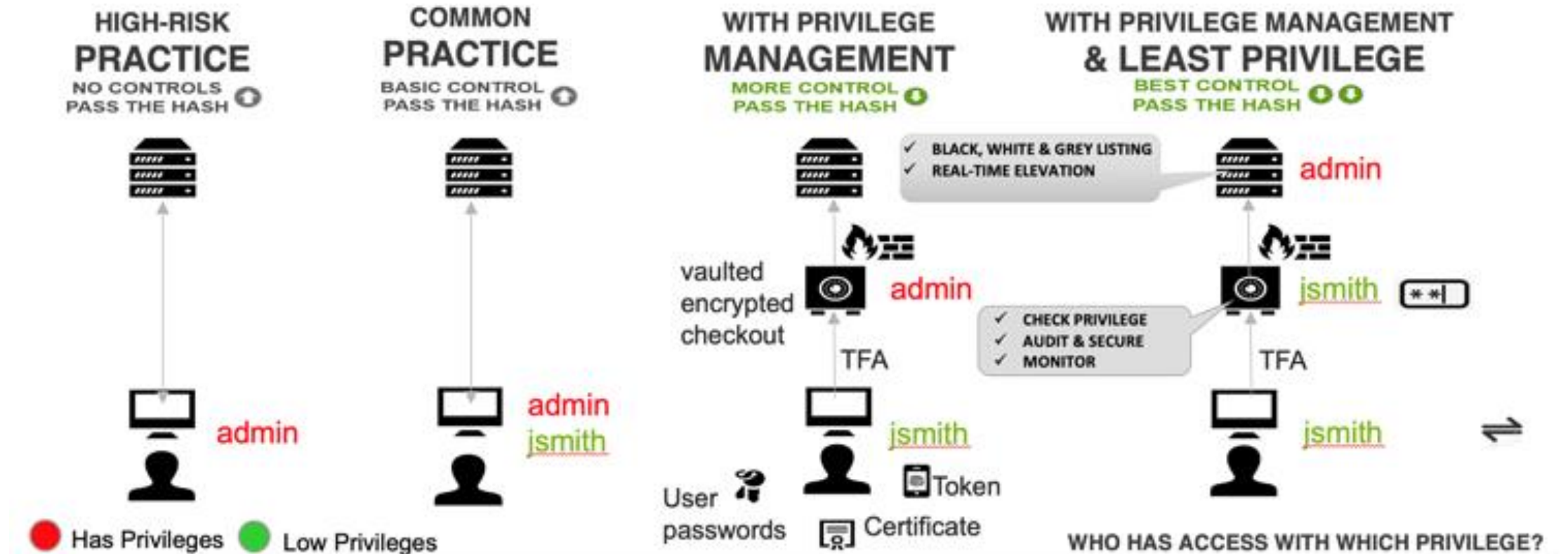
Implications for a lack governance

- Yahoo data breach (2013)
 - 3 billion – real names, email addresses, dates of birth, telephone numbers, and security questions
 - \$350 million estimated loss in value of company
- First American Financial Corporation data breach (2019)
 - 885 million – bank account numbers, bank statements, mortgage and tax records, social security numbers, wire transaction receipts, and driver license images
 - Poor security
- Equifax data breach (2017)
 - 148 million – Social Security numbers, birth dates, addresses, and in some cases driver license numbers and credit card information
 - \$700 million in payouts
- Marriott International data breach (2018)
 - 500 million – combination of contact information, passport number, Starwood Preferred Guest numbers, travel information, credit card numbers and expiration dates, other personal information
 - \$24 million, class-action lawsuits filed
- Facebook data breach (2019)
 - 540 million – phone numbers, user names, genders, and locations

Data Lineage



Principle of Least Privilege



- Vulnerability
- Threat
- Actor
- Attack

Cloud Security – Terms and Concepts

Confidentiality

Integrity

Authenticity

Availability

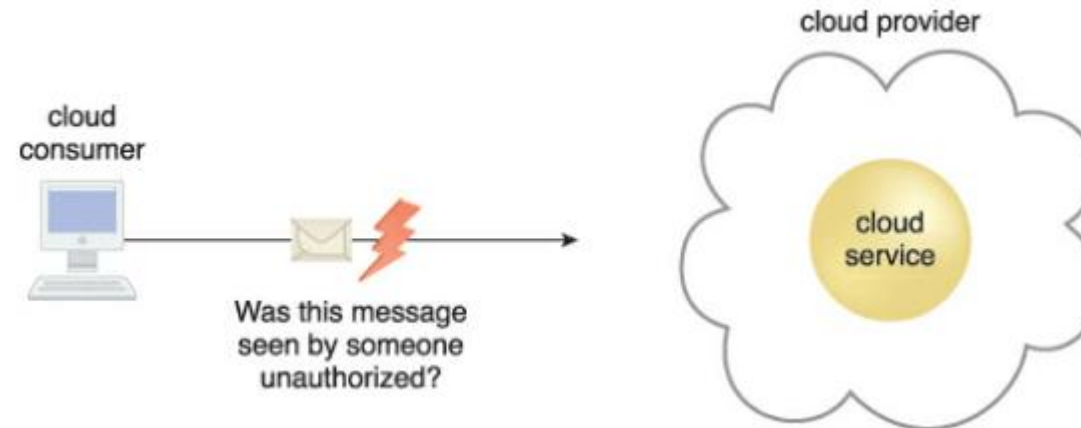
Threat

Vulnerability

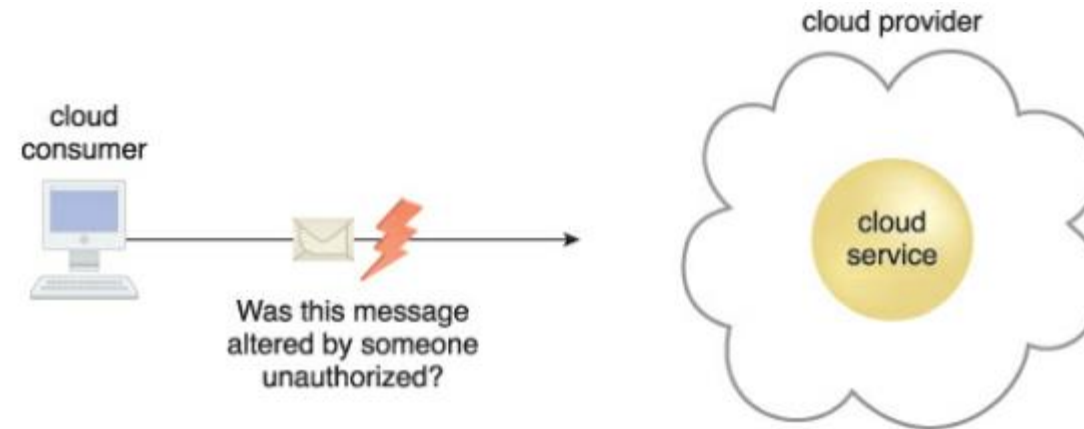
Risk

Security Controls / Mechanisms / Policies

Measuring Security – Confidentiality

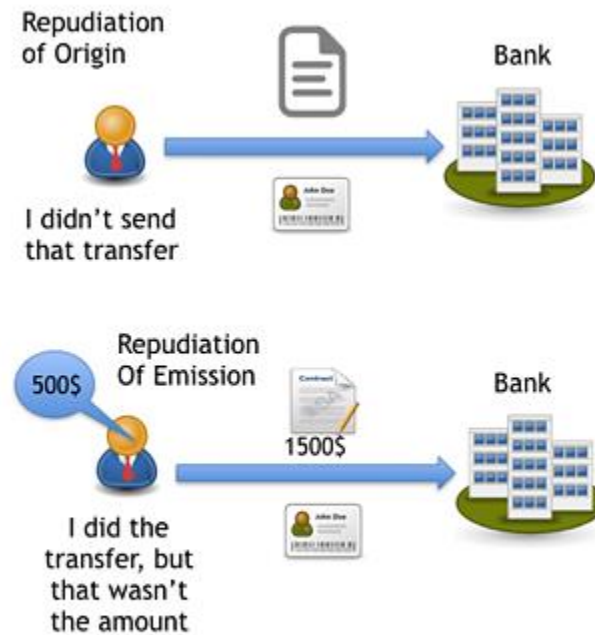


Measuring Security – Integrity



Measuring Security – Authenticity

- Provided by authorised source
- Non repudiation – The inability of party to deny or challenge the authenticity of an interaction



Measuring Security – Availability

- Being accessible and usable during a certain time period
- Responsibility generally shared between Cloud Provider and Carrier.
 - If using Cloud to offer services to 3rd Service Consumers then extends to Cloud Consumer

Lack of Security – Threat & Vulnerability

Threat

- A potential security violation that can breach privacy or cause harm
- Generally exploits a known weakness (vulnerability)

Vulnerability

- A weakness that can be exploited because of insufficient security controls or security controls that have been compromised
 - Configurations deficiencies
 - Security policy weakness
 - User errors
 - Hardware / Firmware flaws
 - Software bugs
 - Poor security architecture

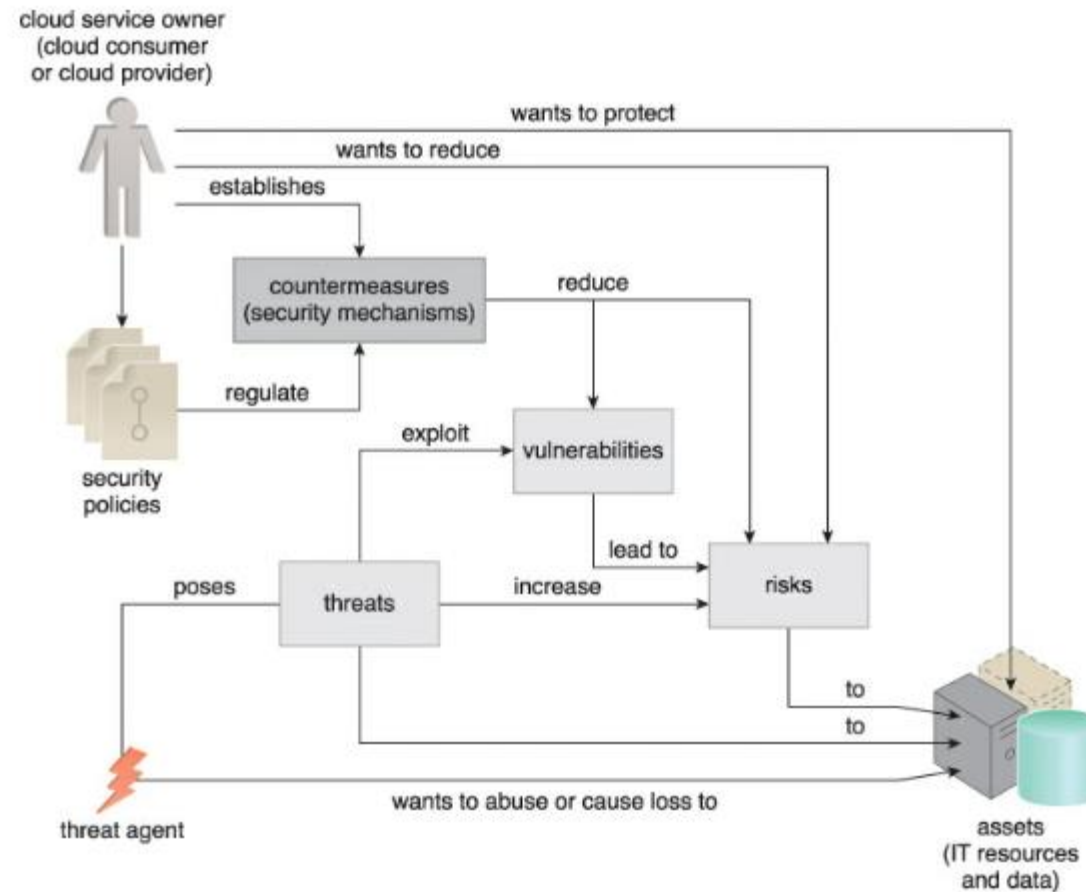
Lack of Security – Risk

- Possibility of loss or harm from an activity
- Measured according to its threat level and the number of possible or known vulnerabilities.
 - The probability of a threat occurring to exploit vulnerabilities in the resource
 - The expectation of loss upon the compromised resource

Improving Security – Controls, Mechanisms, Policies

- Security Controls
 - Countermeasures used to prevent or respond to security threats and to reduce or avoid risk.
- Security Mechanisms
 - Countermeasures are typically described in terms of security mechanisms, which are components comprising a defensive framework
- Security Policies
 - Set of security rules and regulations
 - Definition of how these rules and regulations are implemented and enforced
 - Will direct controls and mechanisms

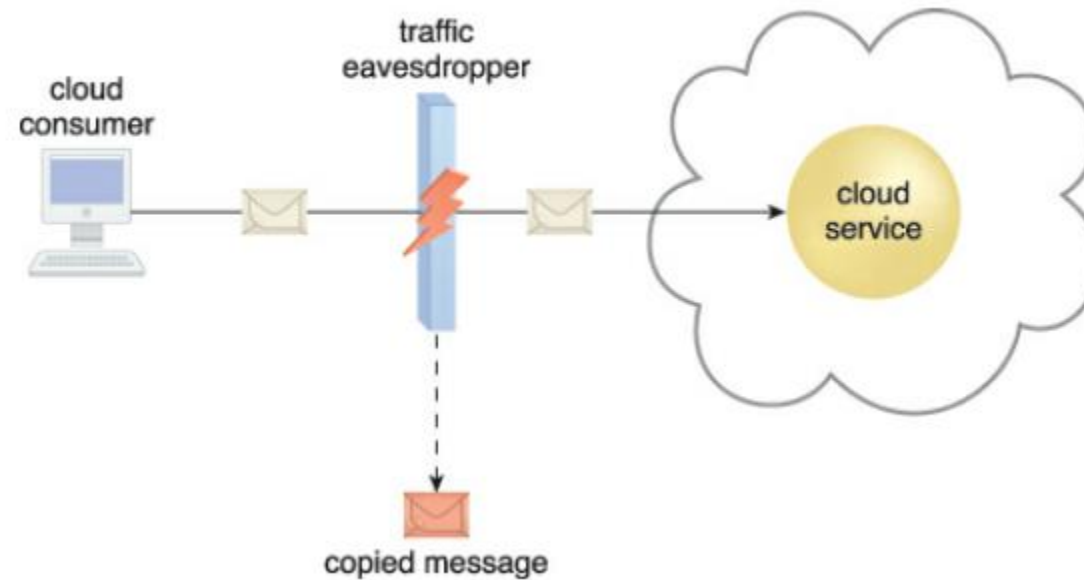
Threat Agents



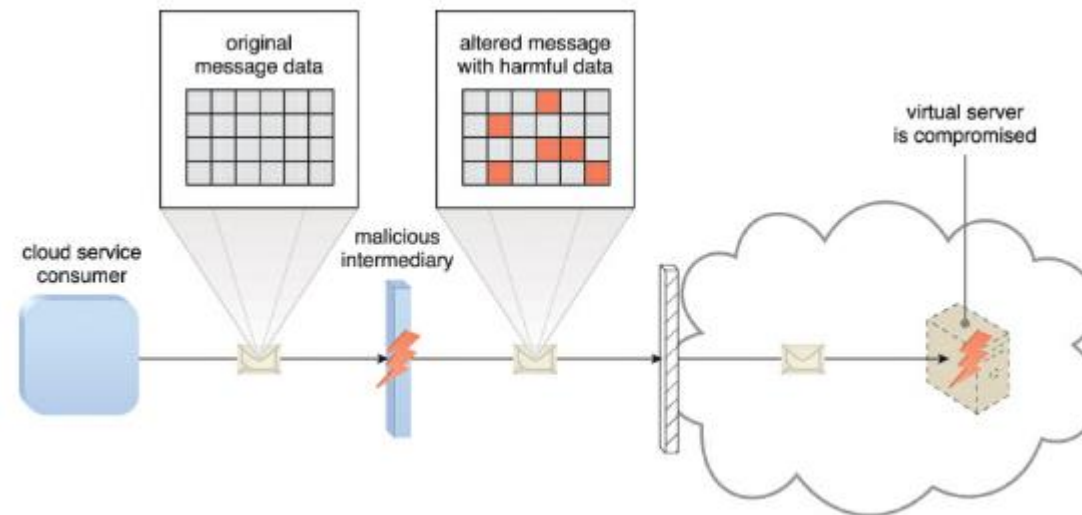
Types of Threat Agents

- Anonymous Attacker
- Malicious Service Agent
- Trusted Attacker
- Malicious Insider

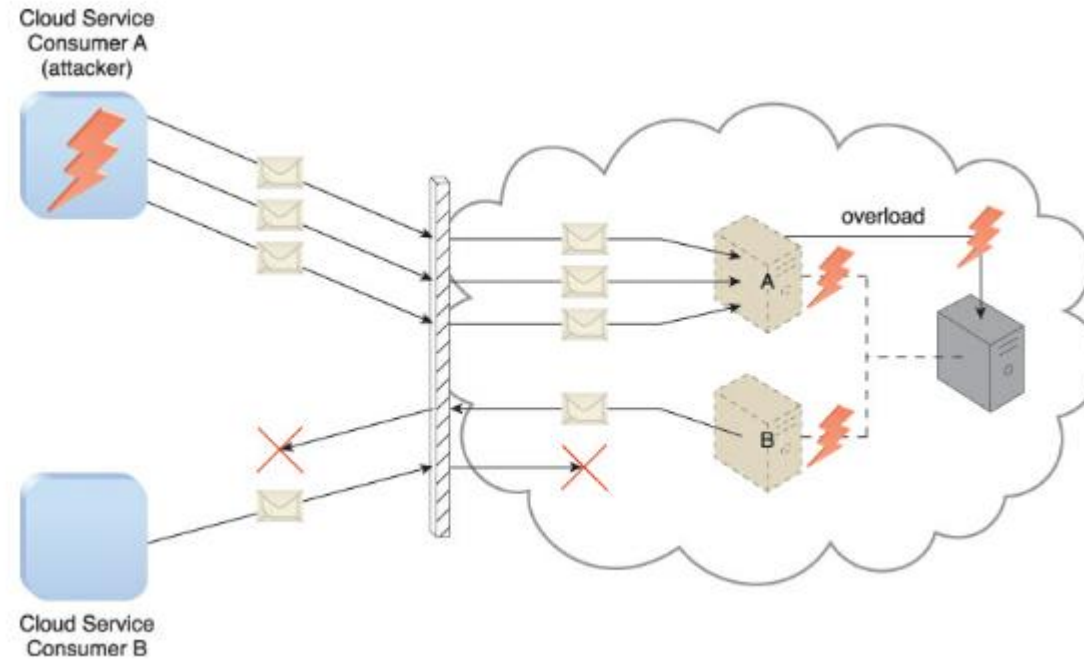
Cloud Security Threats – Traffic Eaves Dropping



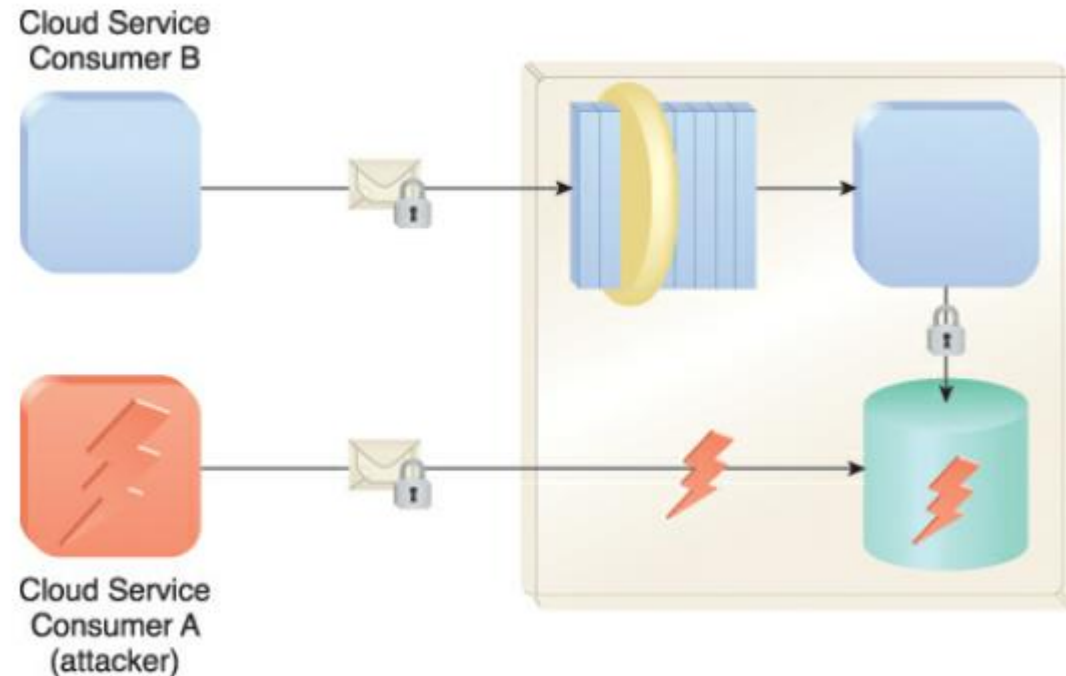
Cloud Security Threats – Malicious Intermediary



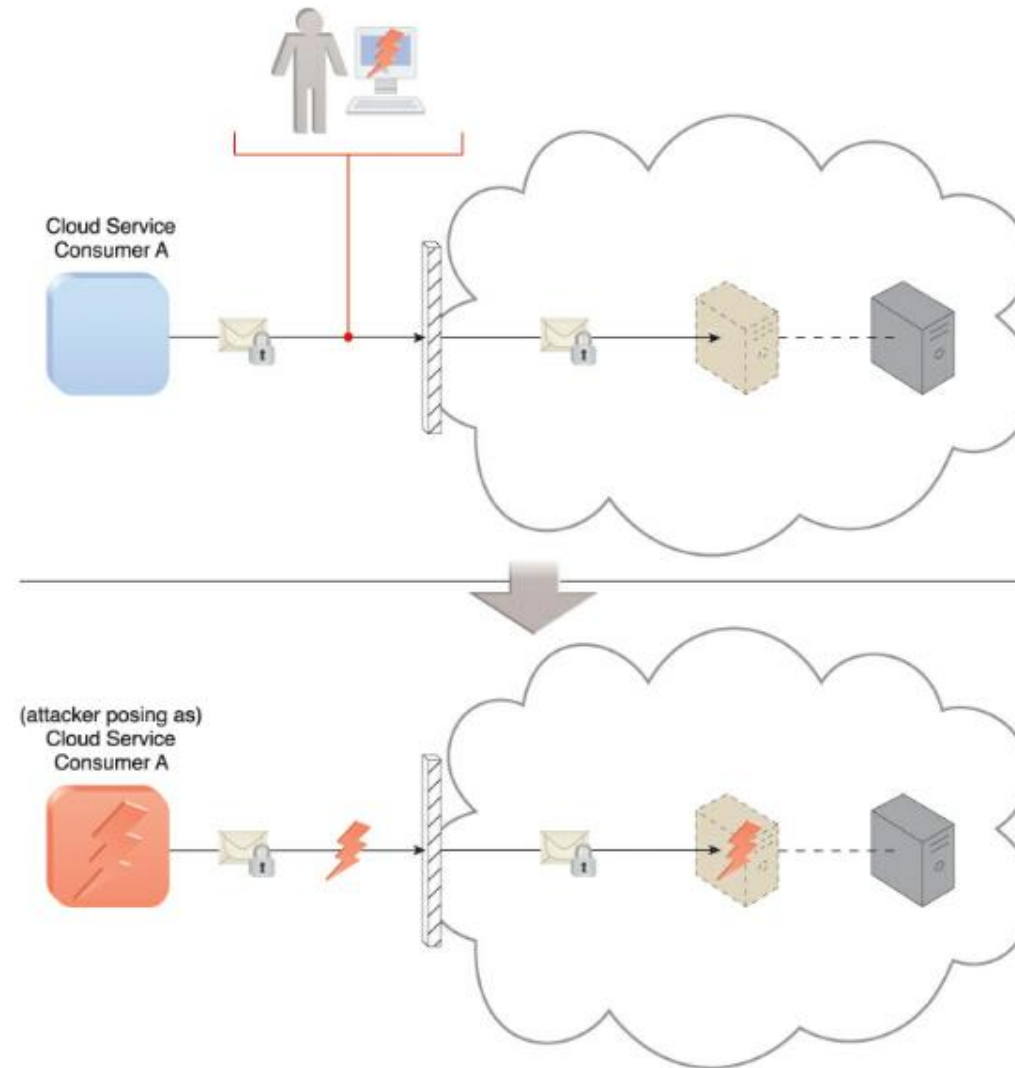
Cloud Security Threats – Denial of Service



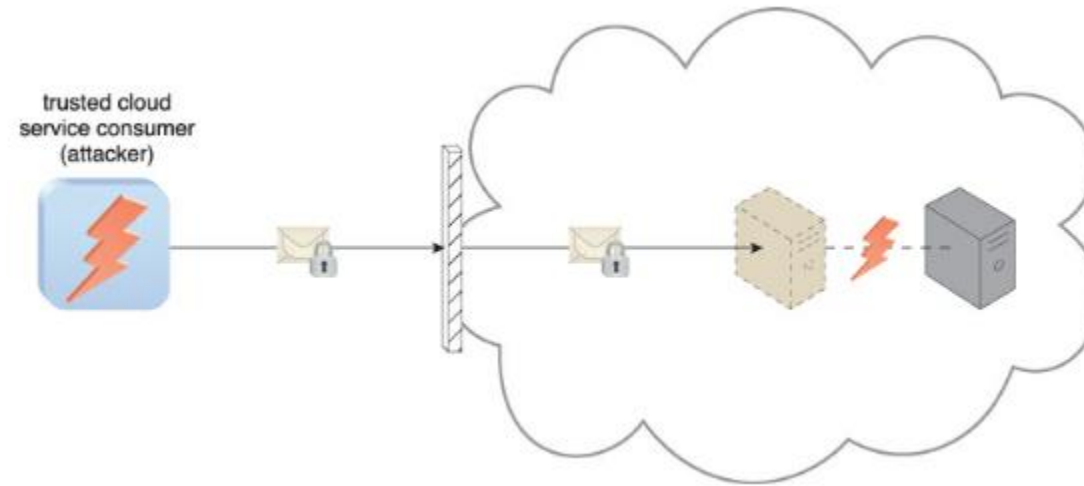
Cloud Security Threats – Insufficient Authorisation



Cloud Security Threats – Impersonation



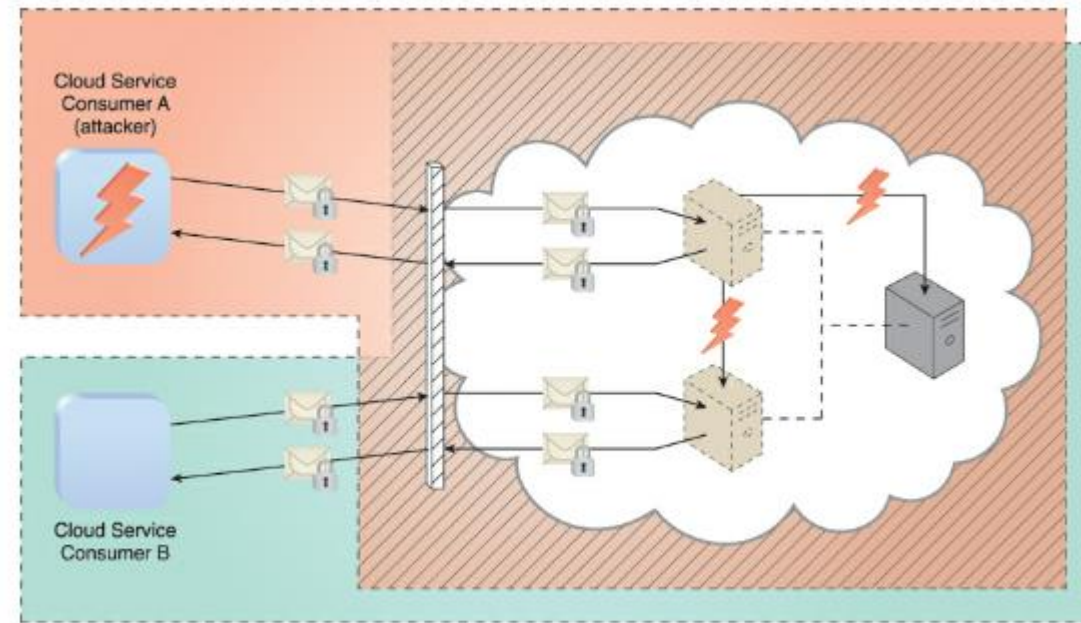
Cloud Security Threats – Virtualisation Attack



Container Attacks

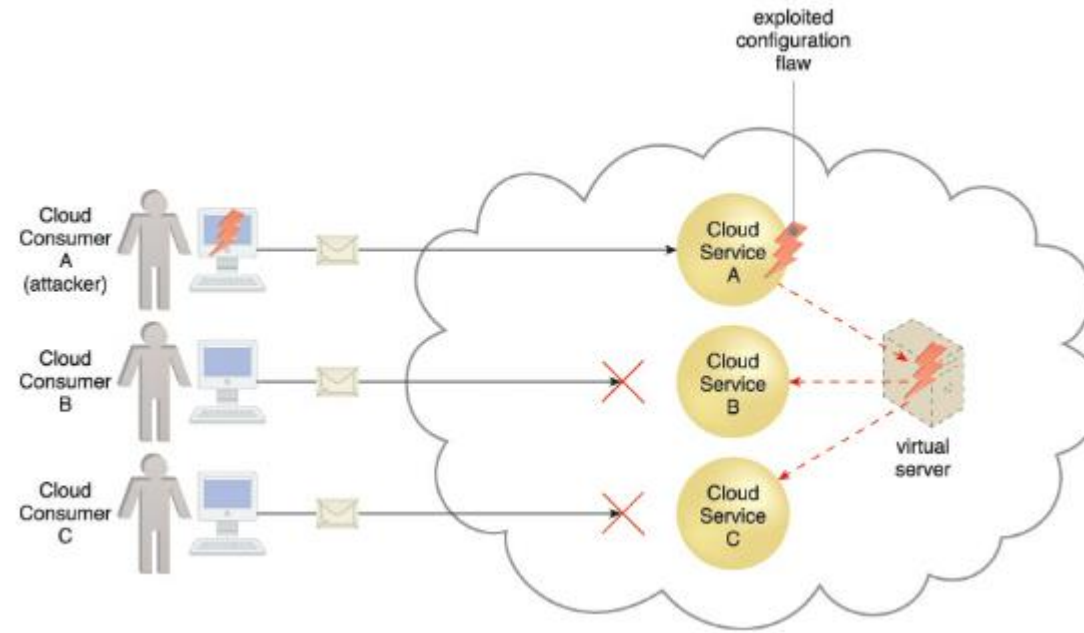
- Containerisation introduces a lack of isolation from the host operating system
 - Create containers within the OS so that if compromised only those containers have issues
 - One service per physical server model – Reduces risk but increases resource usage thus cost and complexity

Cloud Security Threats – Overlapping Trust Boundaries



Other considerations

- Poorly implemented cloud service deployment

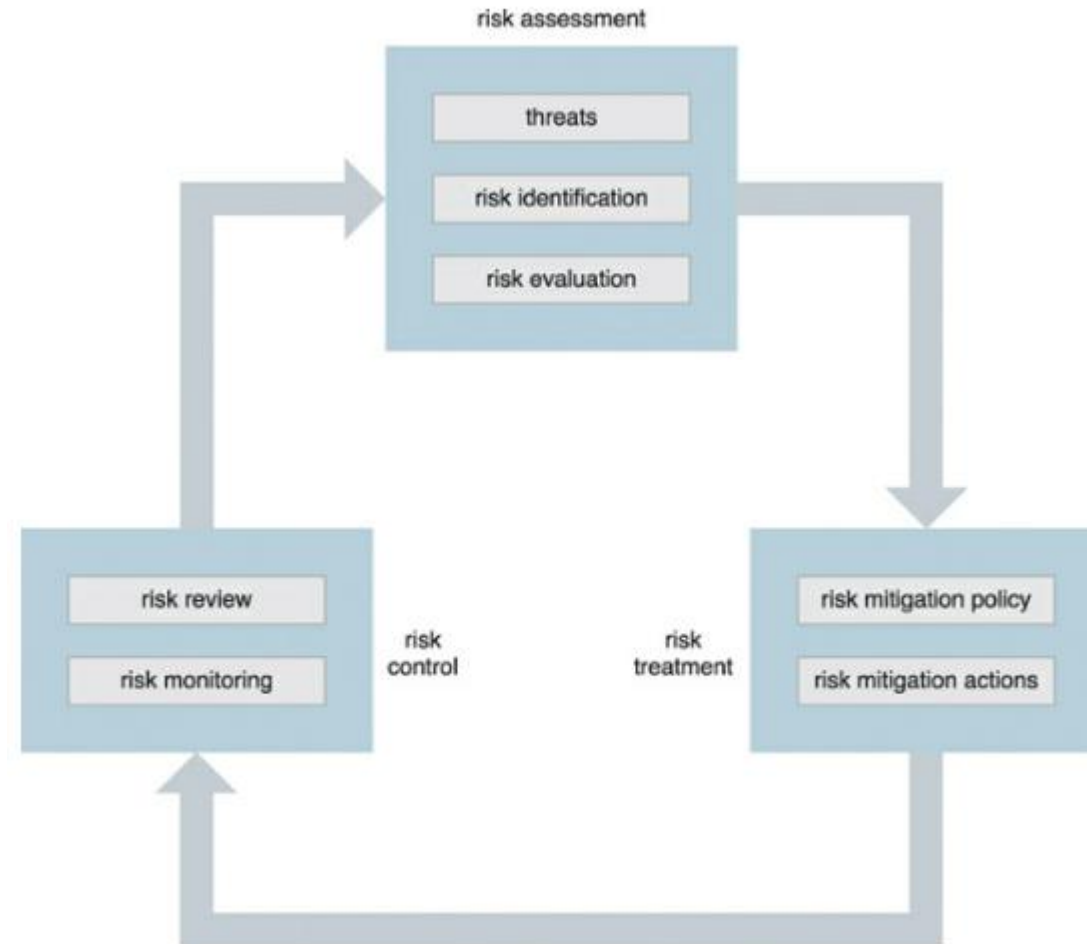


Other considerations

- Incompatibilities in security policies
- Cloud contracts
 - Where does the liability lie?
 - What is the level of indemnity?
 - The greater the risk absorbed by the provider the less to bear by the consumer
 - What are the lines responsibilities in a shared model? IaaS vs. SaaS

Risk Management

- Probability of Occurrence
- Impact of Occurrence



Risk Assessment Matrix

| | | Risk Assessment Matrix | | | |
|-------------|----------------|------------------------|--------------|--------------|----------------|
| | | Severity | | | |
| | | Catastrophic - 4 | Critical - 3 | Marginal - 2 | Negligible - 1 |
| | | | | | |
| Probability | Frequent - 4 | High (16) | High (12) | Serious (8) | Medium (4) |
| | Probable - 3 | High (12) | Serious (9) | Serious (6) | Medium (3) |
| | Remote - 2 | Serious (8) | Serious (6) | Medium (4) | Low (2) |
| | Improbable - 1 | Medium (4) | Medium (3) | Low (2) | Low (1) |

Cloud Security – Security Mechanisms

Encryption

Hashing

Digital Signatures

Public Key Infrastructure (PKI)

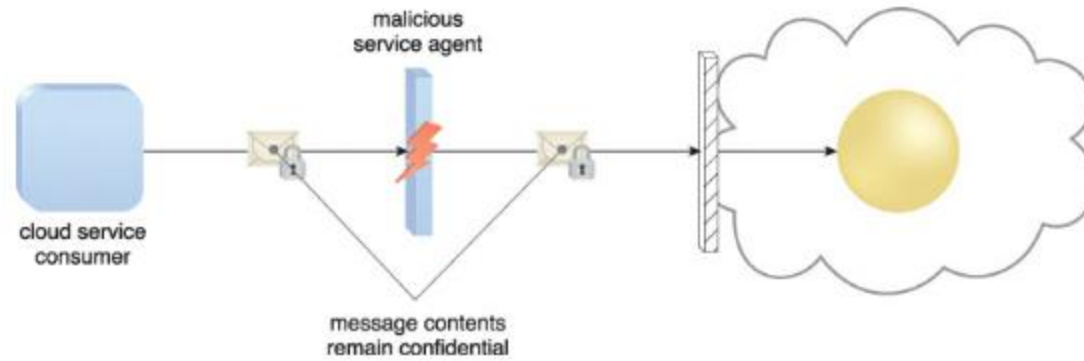
Identity and Access Management (IAM)

Single Sign On

Cloud Based Security Groups

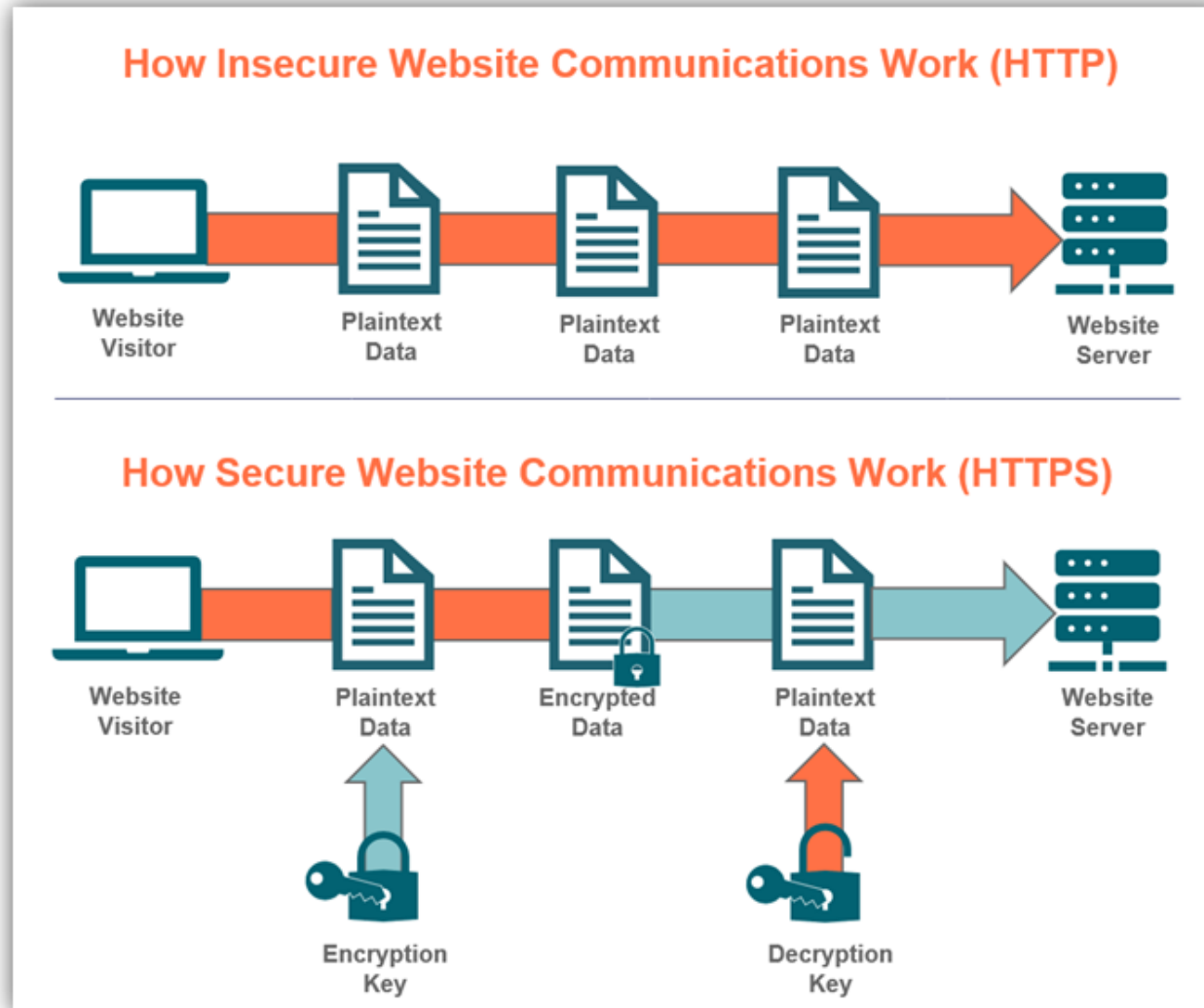
Hardening

Encryption



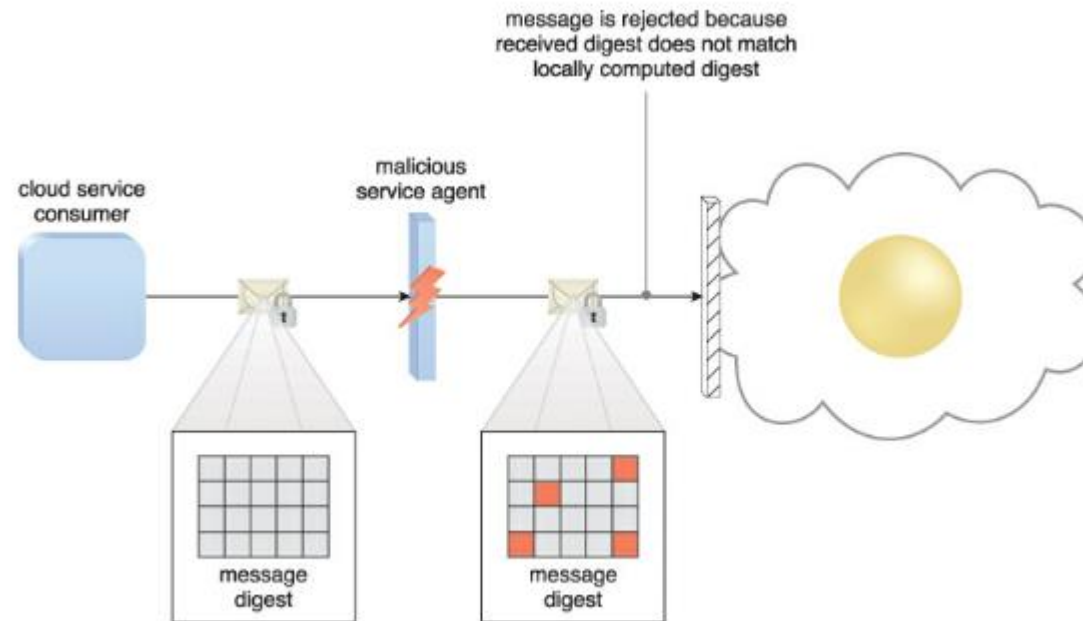
HTTPS

- Ensure message confidentiality through encryption

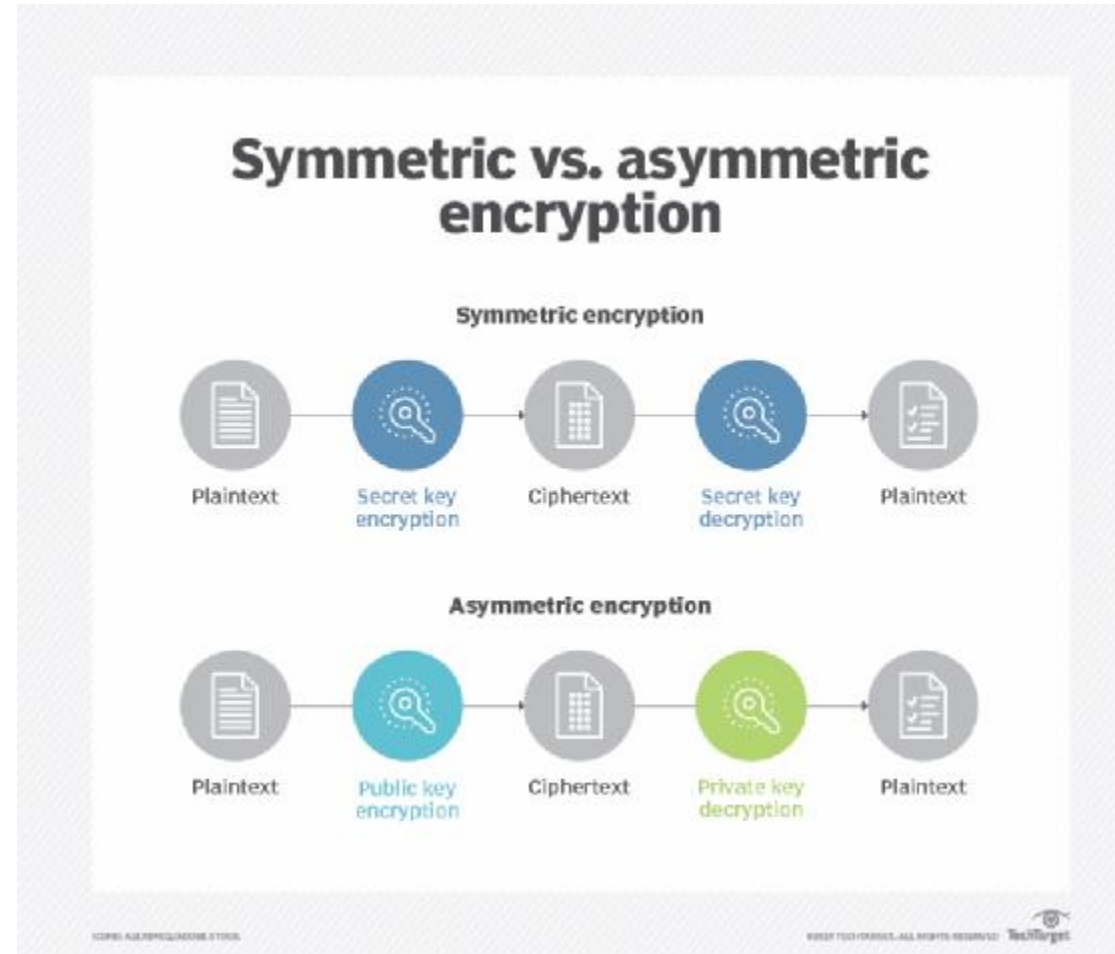


Hashing

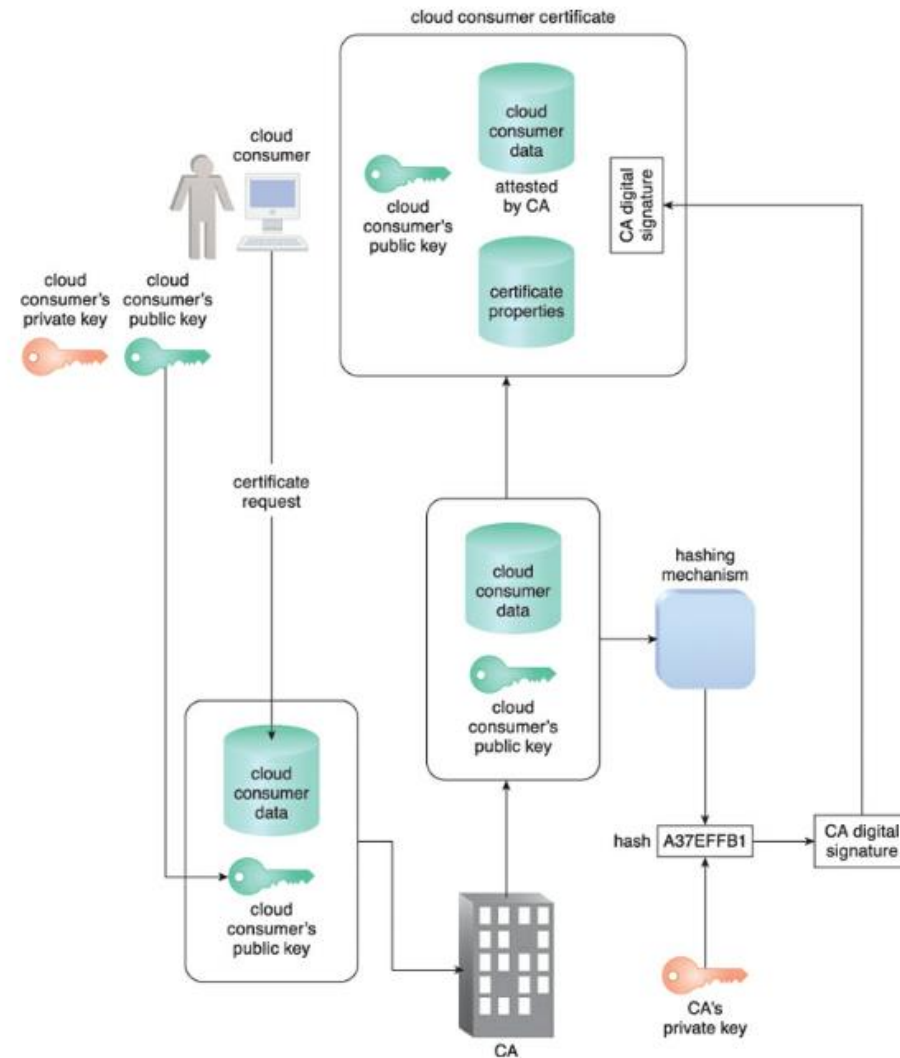
MD5 / SHA 1 – 3, generally use SHA2



Symmetric / Asymmetric Encryption



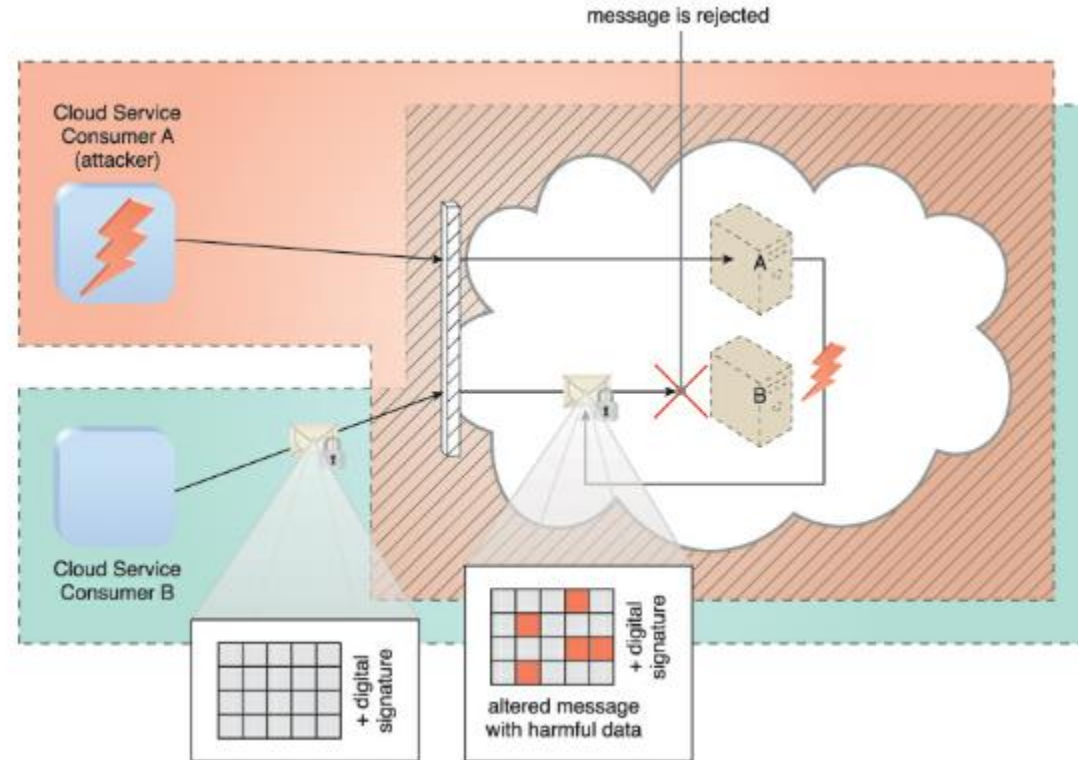
Public Key Infrastructure (PKI)



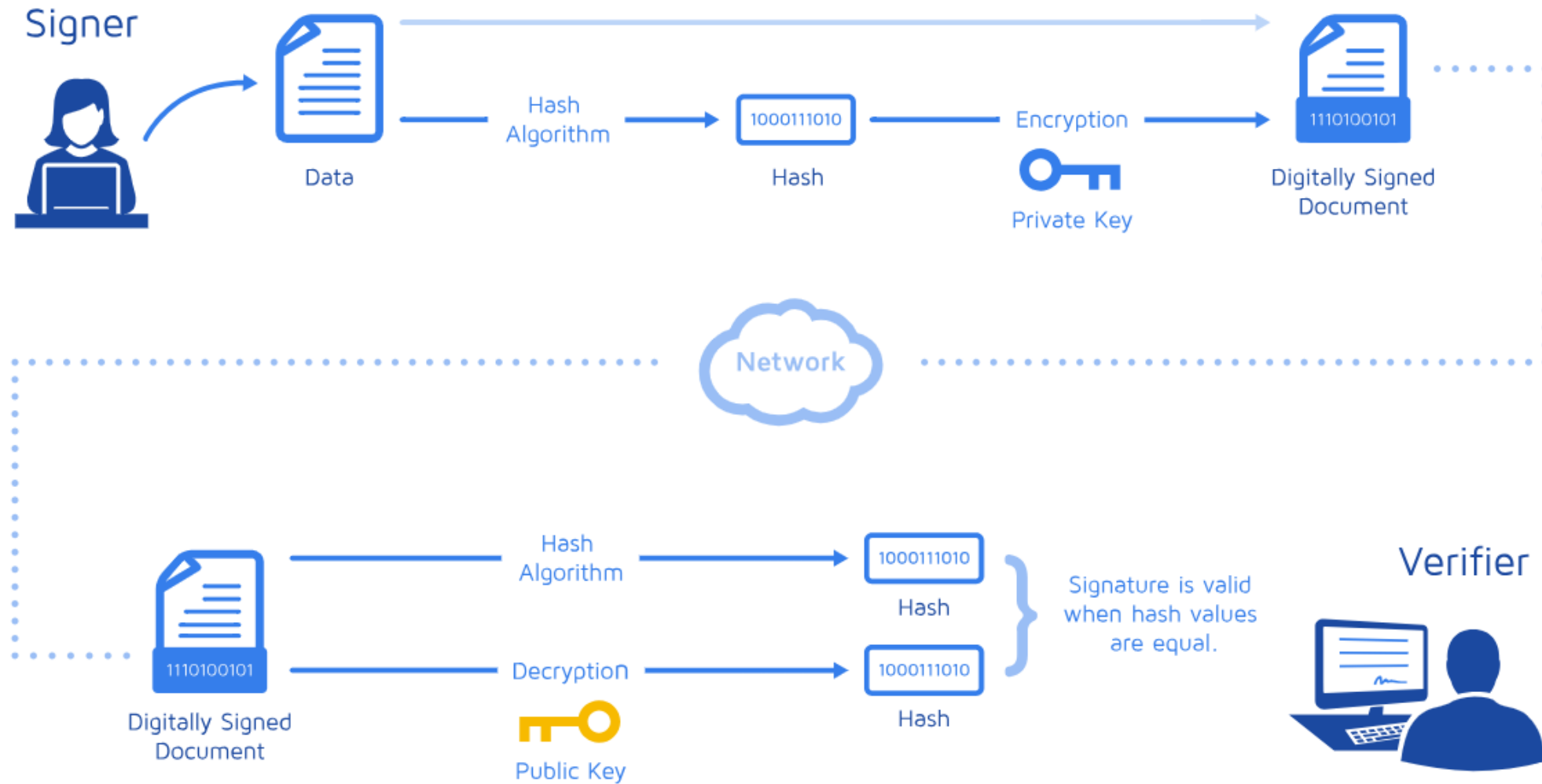
Secure Communication Between 2 People (PKI)

- Alice and Bob want to exchange a message securely
- Both Alice and Bob have a public key and a private key (a
 - Public keys are available to anyone
 - Private keys are kept private
 - If a message is encrypted with a public key then it can only be decrypted by the private key, similar to a lock and a key
- Imagine Alice and Bob are exchanging a locked box with a message:
 1. **Alice** puts a message in a box and locks it with **Bob's public lock (key)**. Only Bob can open this box with his private key.
 2. To prove it's from her, **Alice** also seals the box with her own private seal (signature).
 3. **Bob** receives the box. He checks Alice's seal using her public key to ensure it's really from her and hasn't been tampered with.
 4. Once verified, **Bob** uses his private key to unlock the box and read the message.

Digital Signing



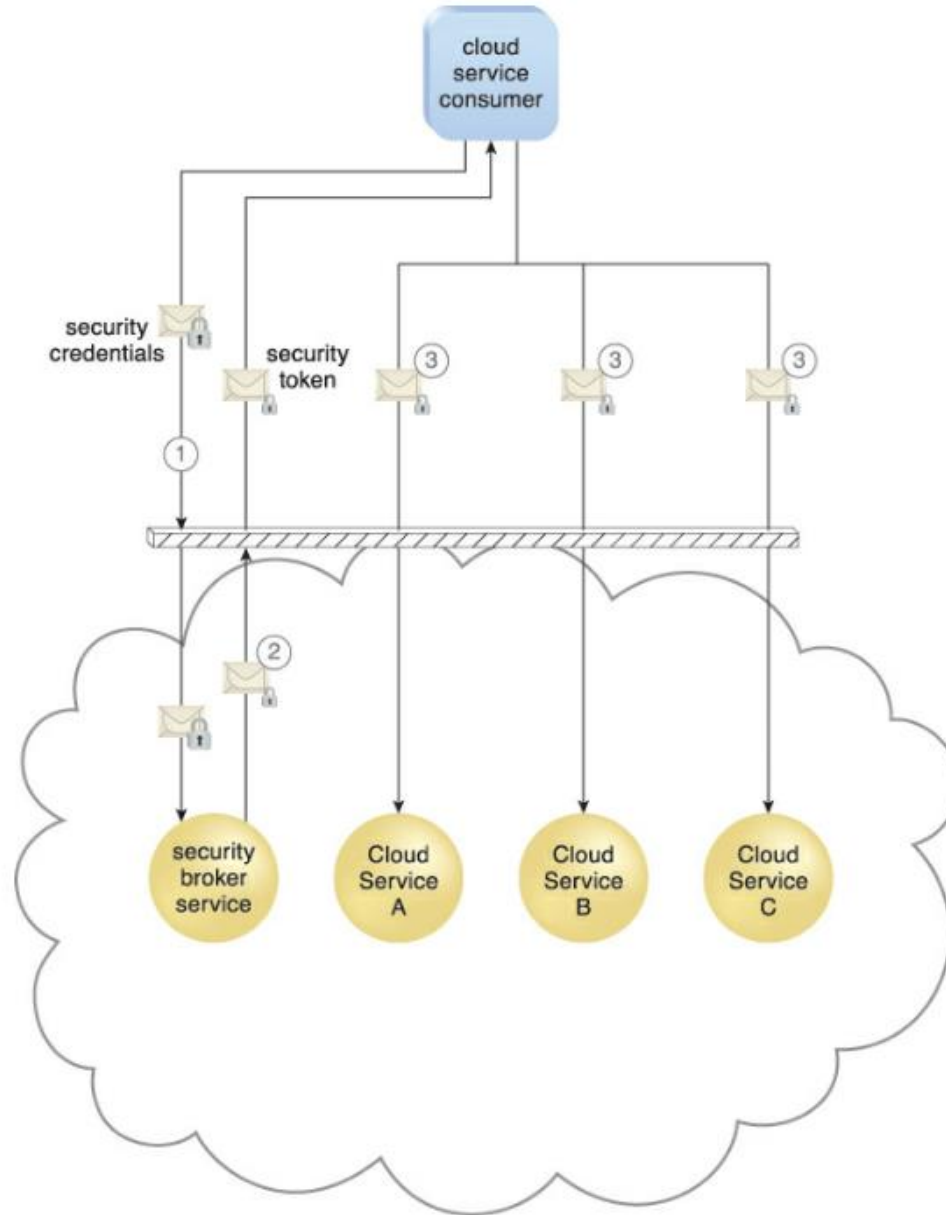
How Digital Signing Works



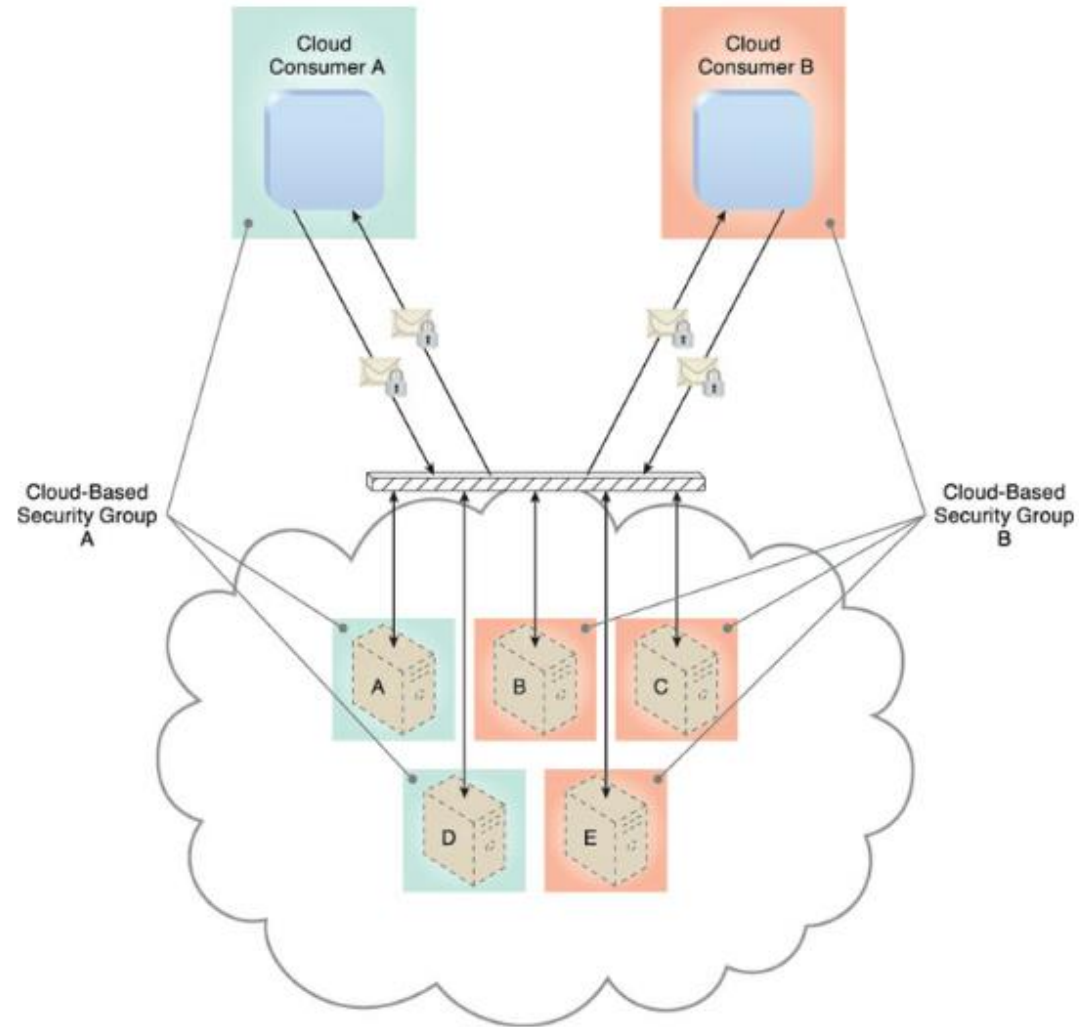
Identity Access Management (IAM)

- Authentication
- Authorisation
- User Management
 - User identities
 - Access groups
 - Managing identities
 - Password policies
 - Role / privilege management
- Credential Management
- Counter insufficient authorization, denial of service, overlapping trust boundaries, virtualization and containerization attack threats.

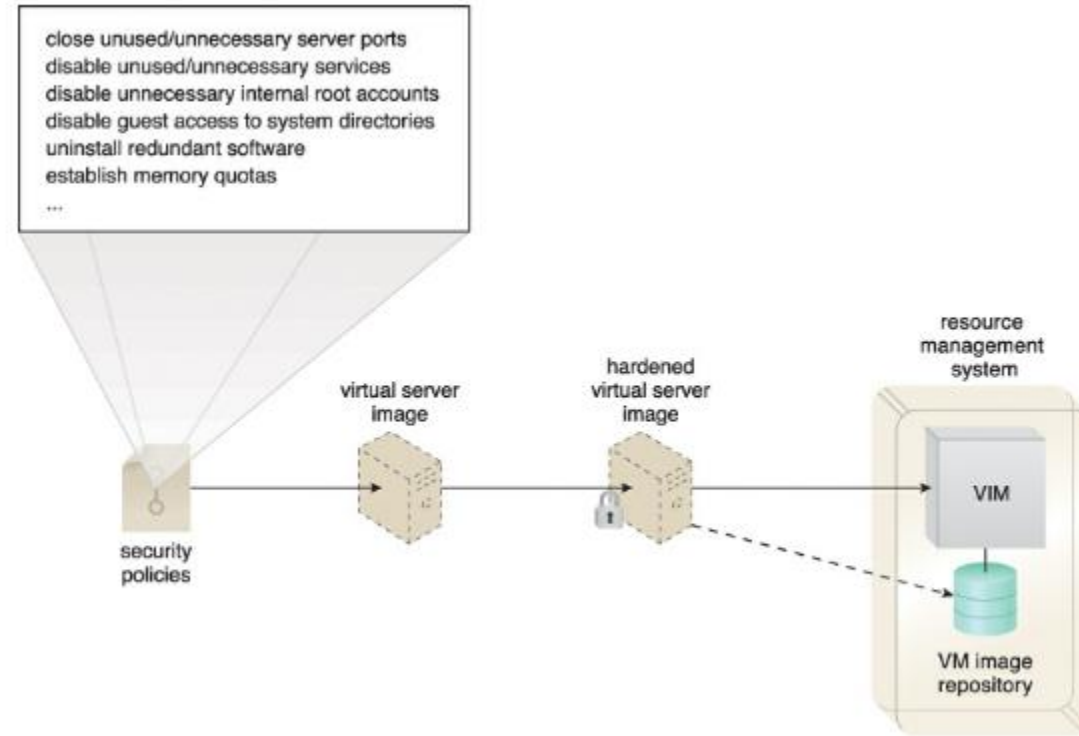
Single Sign On



Cloud Based Security Groups



Hardening



Thank you



LA TROBE
UNIVERSITY

Centre for
Data Analytics
and Cognition

http



LinkedIn



g Scholar

