RSAConference™2024
San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: IDY-R05

The Storm-0558 Attack

Inside Microsoft Identity Security's Response

#RSAC

Alex Weinert
Vice President, Identity Security
Microsoft Corporation

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference™2024
San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: IDY-R05

The Storm-0558 Attack

(most recent attack)

Inside Microsoft Identity Security's Response

#RSAC

Alex Weinert
Vice President, Identity Security
Microsoft Corporation

Cyber Libs

The _____ Attack
(most recent attack)

Inside Microsoft Identity Security's Response

In _____, _____-based actor _____ successfully
(month and year) *(nation state)* *(type of threat)*

_____ to access _____ in _____ using
(threat action) *(sensitive resource)* *(target)*

_____. This session will walk you through the insider's
(attack vector)

view of the attack, investigation, mitigation, and repairs resulting from this attack with a focus on what worked and what didn't when defending against this _____.
(type of threat)

Cyber Libs

The Storm-0558 Attack
(most recent attack)

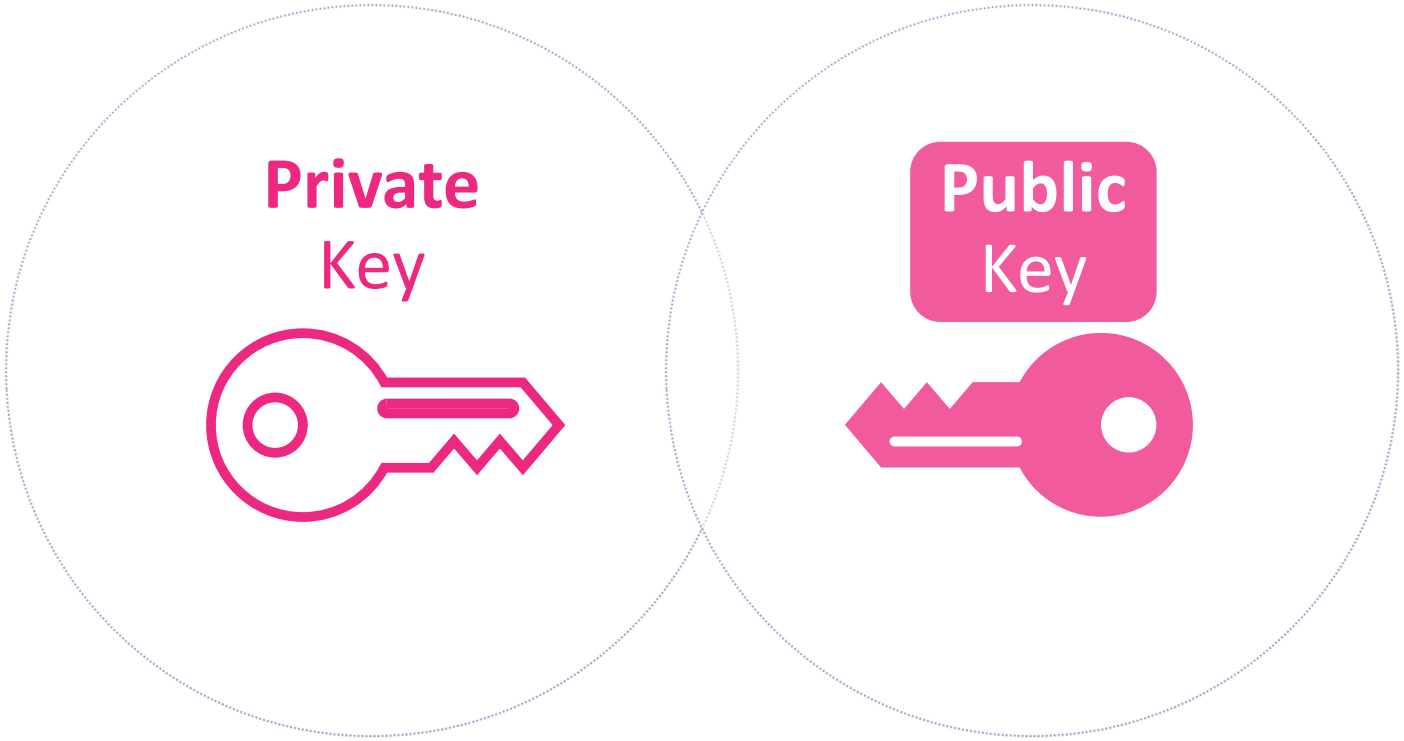
Inside Microsoft Identity Security's Response

In June 2023 *(month and year)*, China *(nation state)*-based actor Storm-0558 *(type of threat)* successfully Forged tokens *(threat action)* to access customer email *(sensitive resource)* in 22 agencies *(target)* using an acquired signing key *(attack vector)*. This session will walk you through the insider's view of the attack, investigation, mitigation, and repairs resulting from this attack with a focus on what worked and what didn't when defending against this APT actor *(type of threat)*.

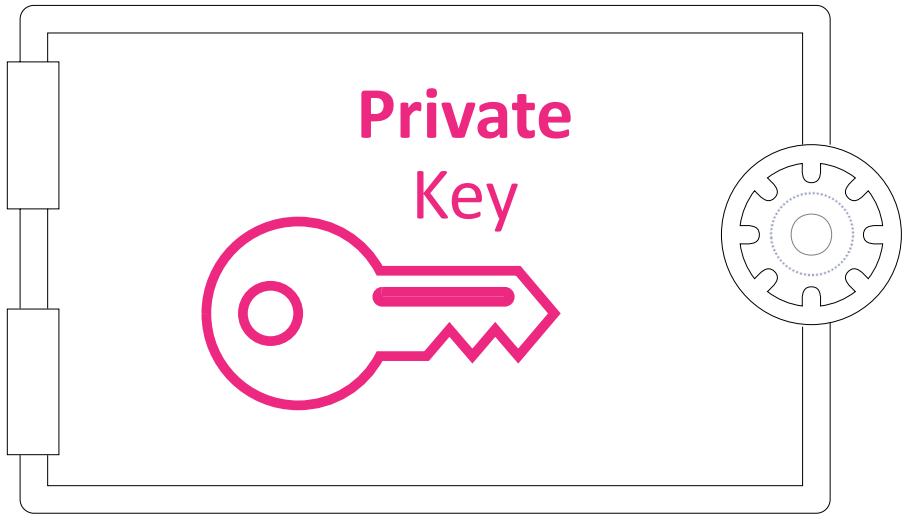
A Crime Story

The scene

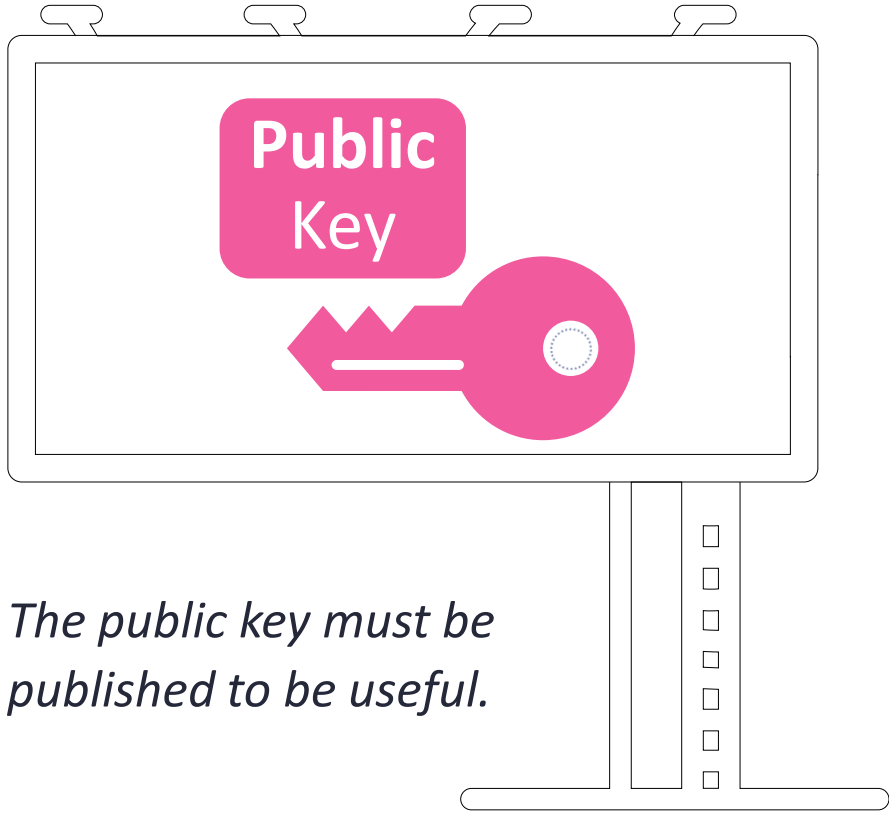
Public Key Cryptography



Public Key Cryptography

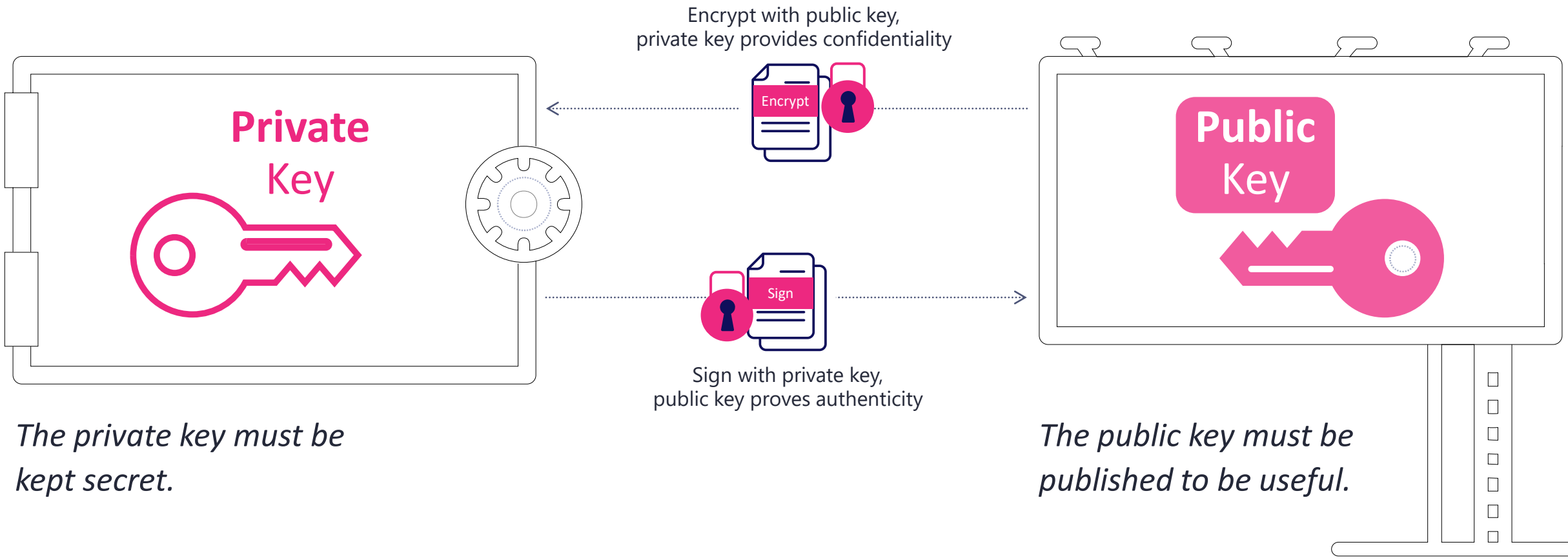


The private key must be kept secret.



The public key must be published to be useful.

Public Key Cryptography



The private key must be kept secret.

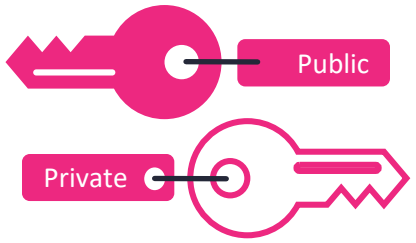
The public key must be published to be useful.

Public Key Cryptography

Using key pairs to prove authenticity

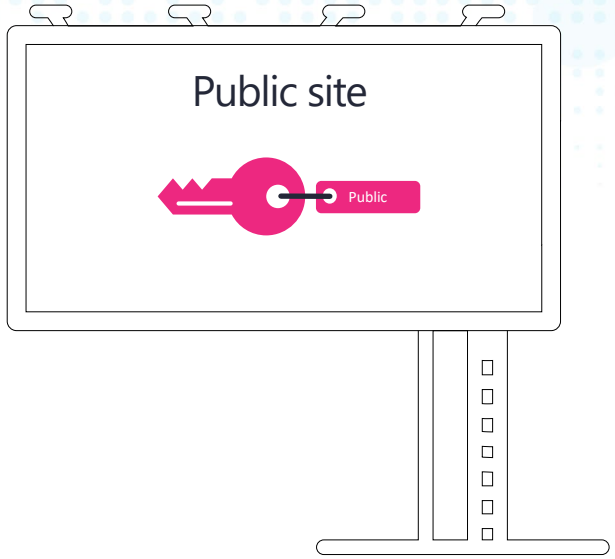
Public Key Cryptography

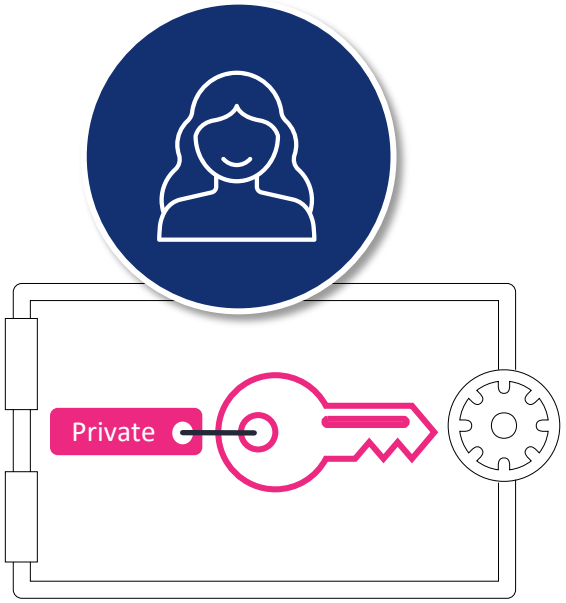
Using key pairs to prove authenticity



Public Key Cryptography

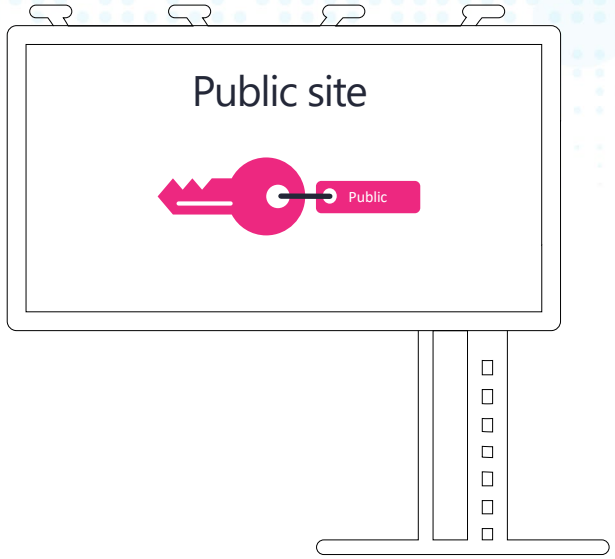
Using key pairs to prove authenticity

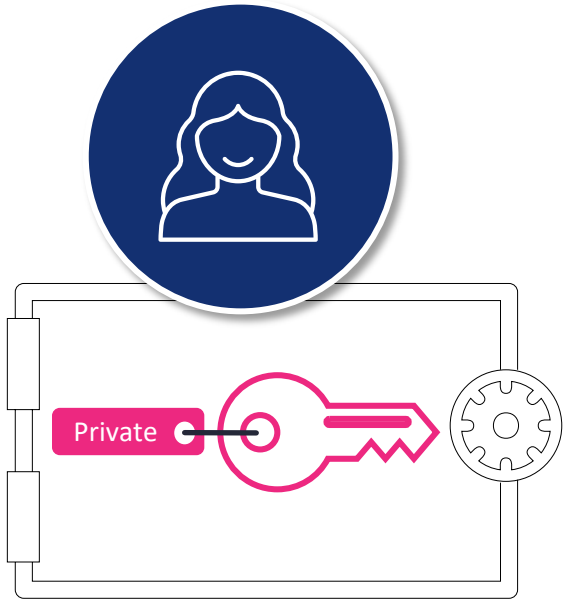




Public Key Cryptography

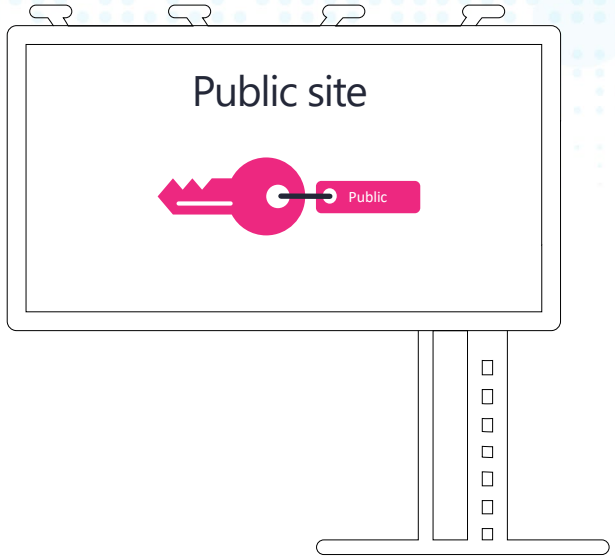
Using key pairs to prove authenticity

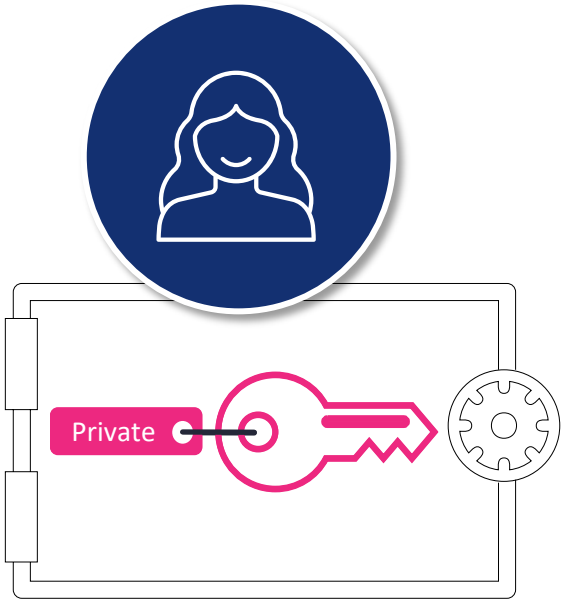




Public Key Cryptography

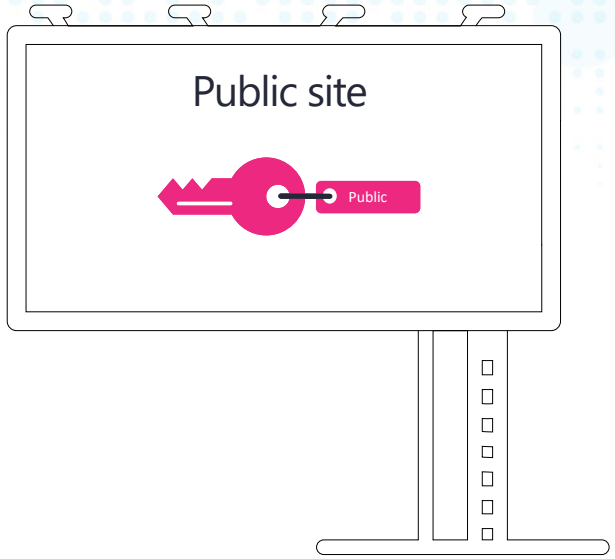
Using key pairs to prove authenticity

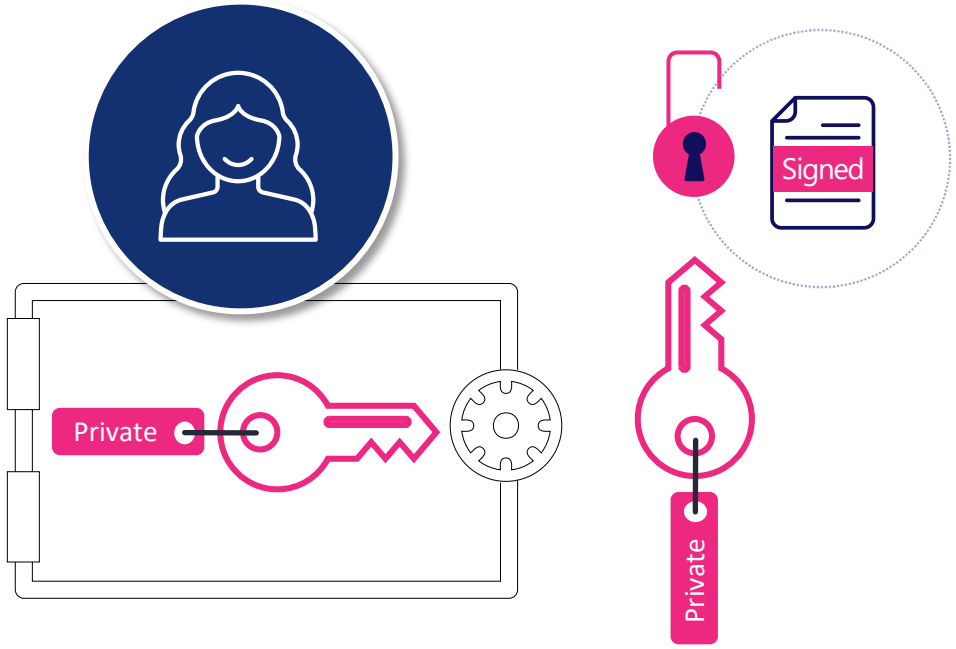




Public Key Cryptography

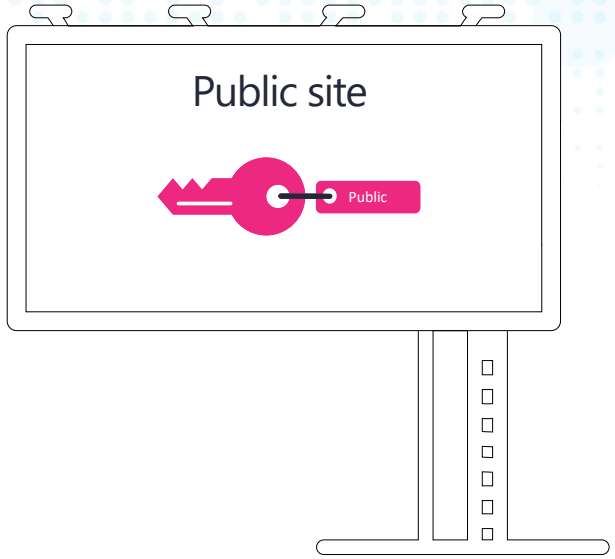
Using key pairs to prove authenticity

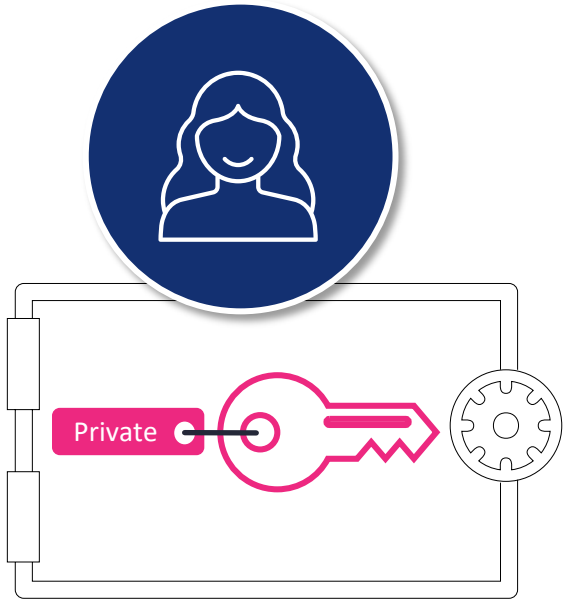




Public Key Cryptography

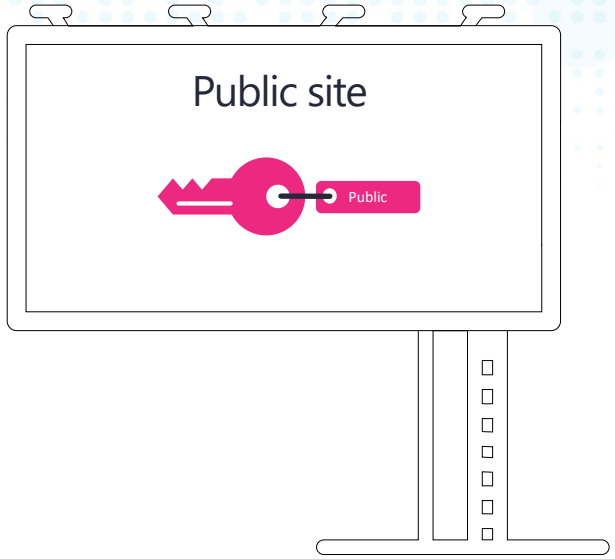
Using key pairs to prove authenticity

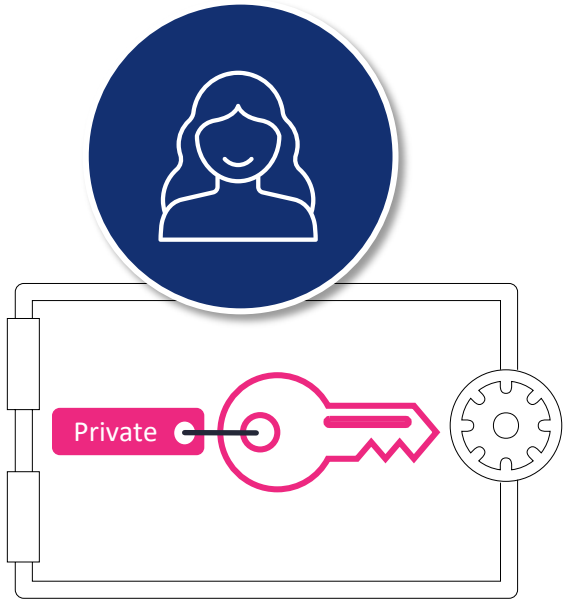




Public Key Cryptography

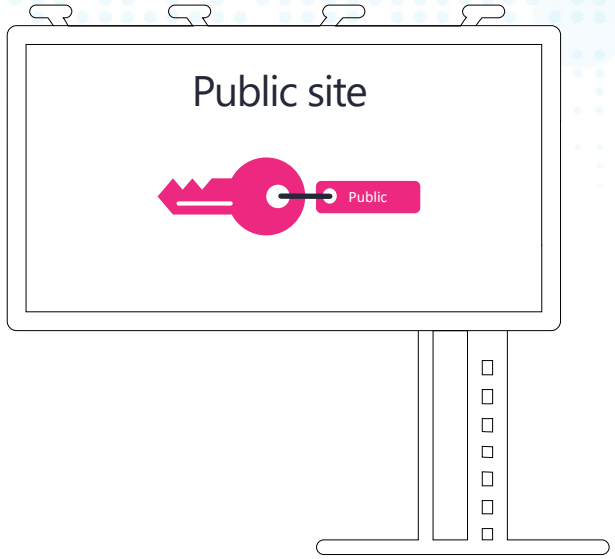
Using key pairs to prove authenticity

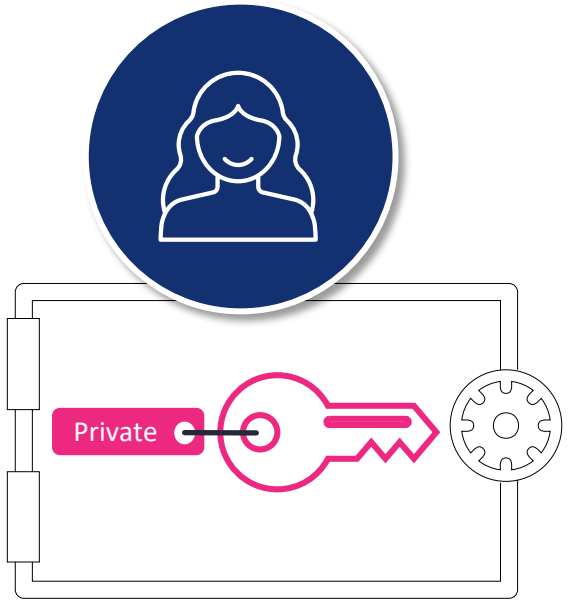




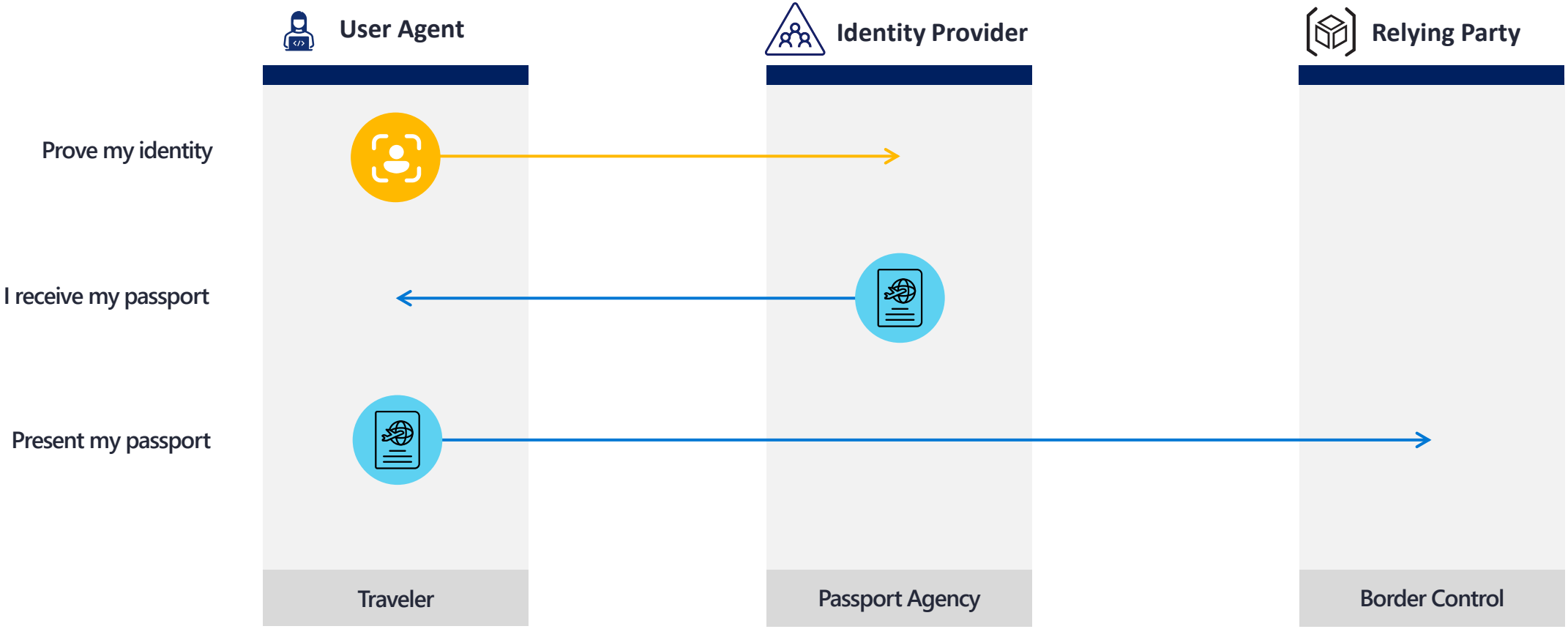
Public Key Cryptography

Using key pairs to prove authenticity

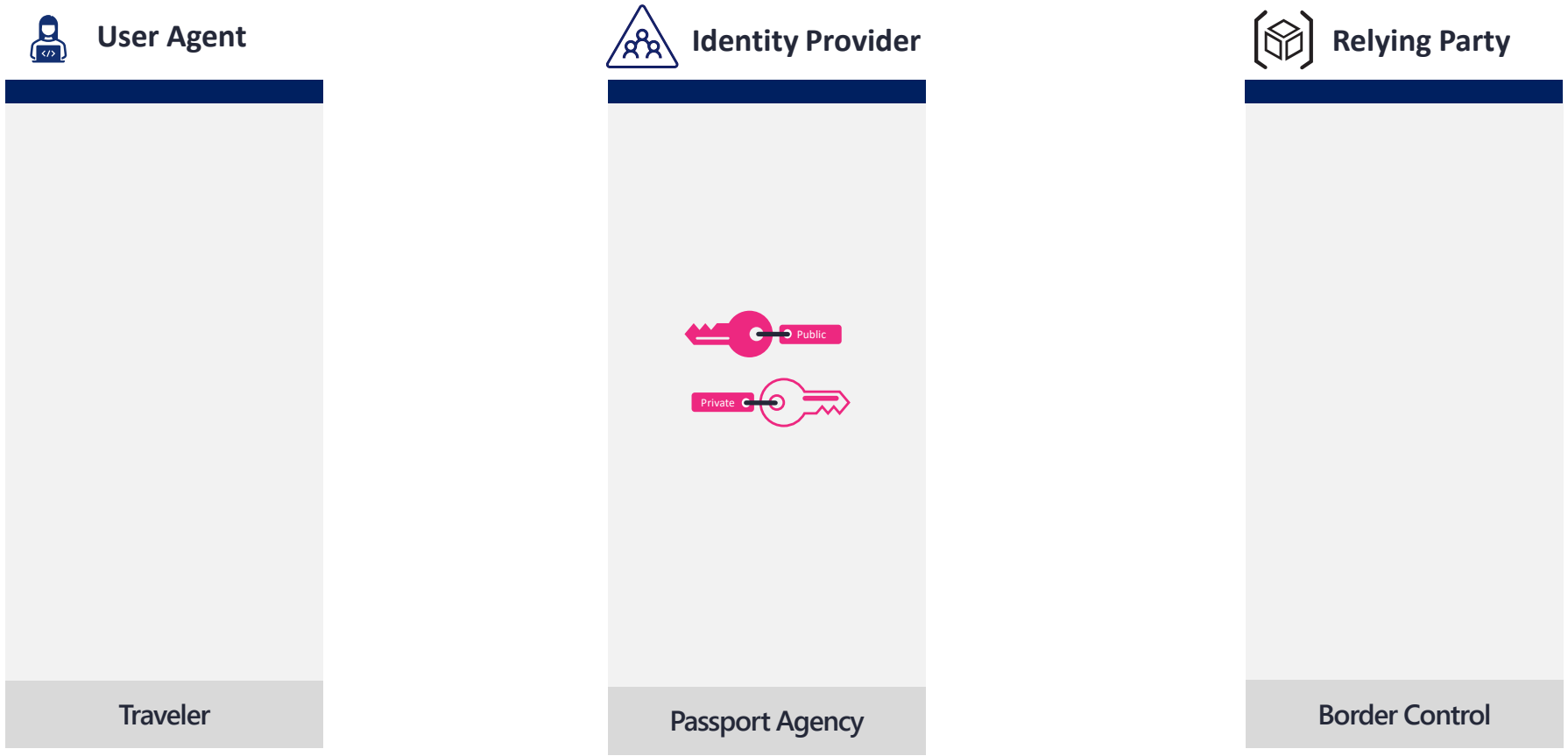




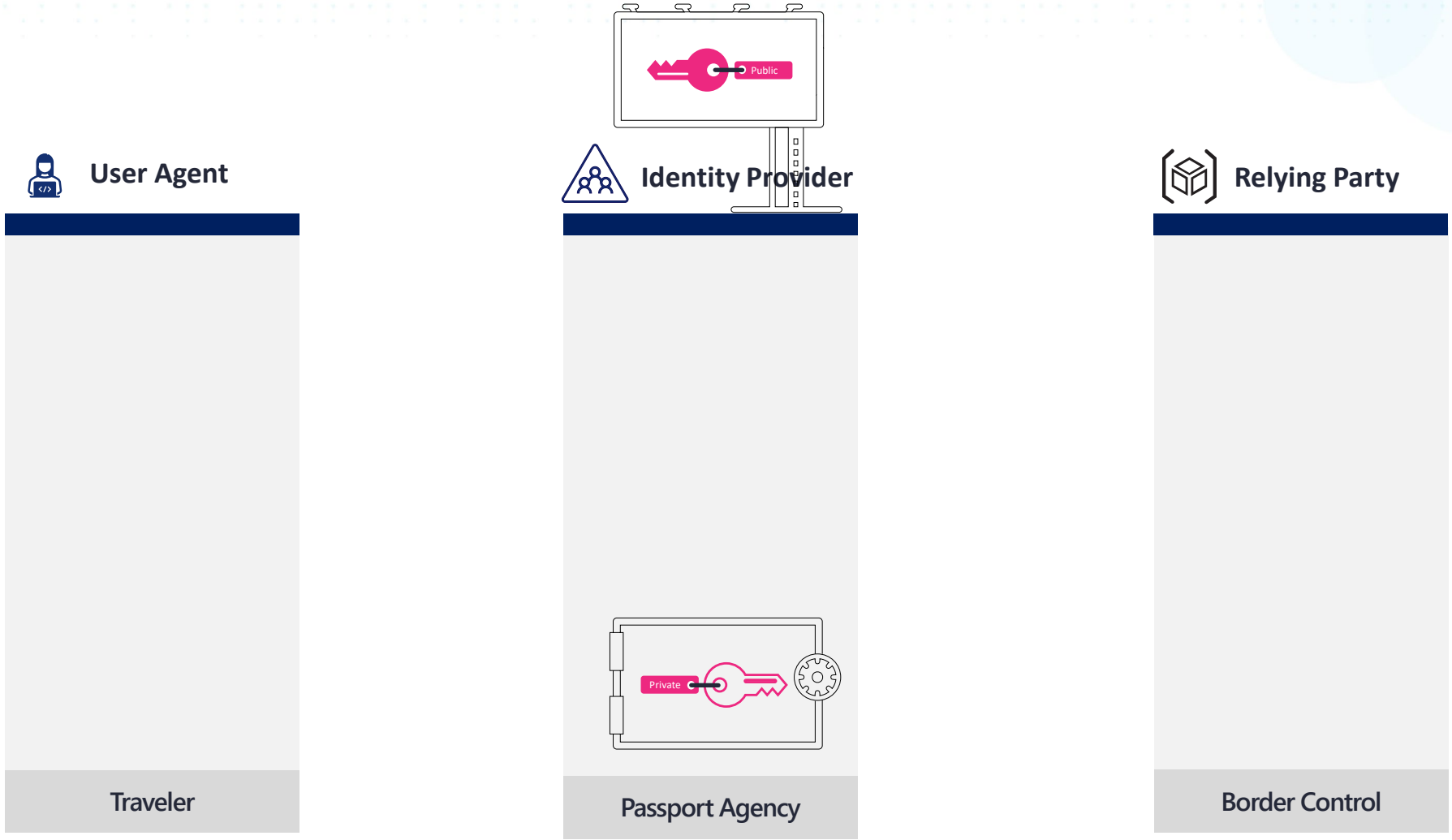
Single Sign-on basics



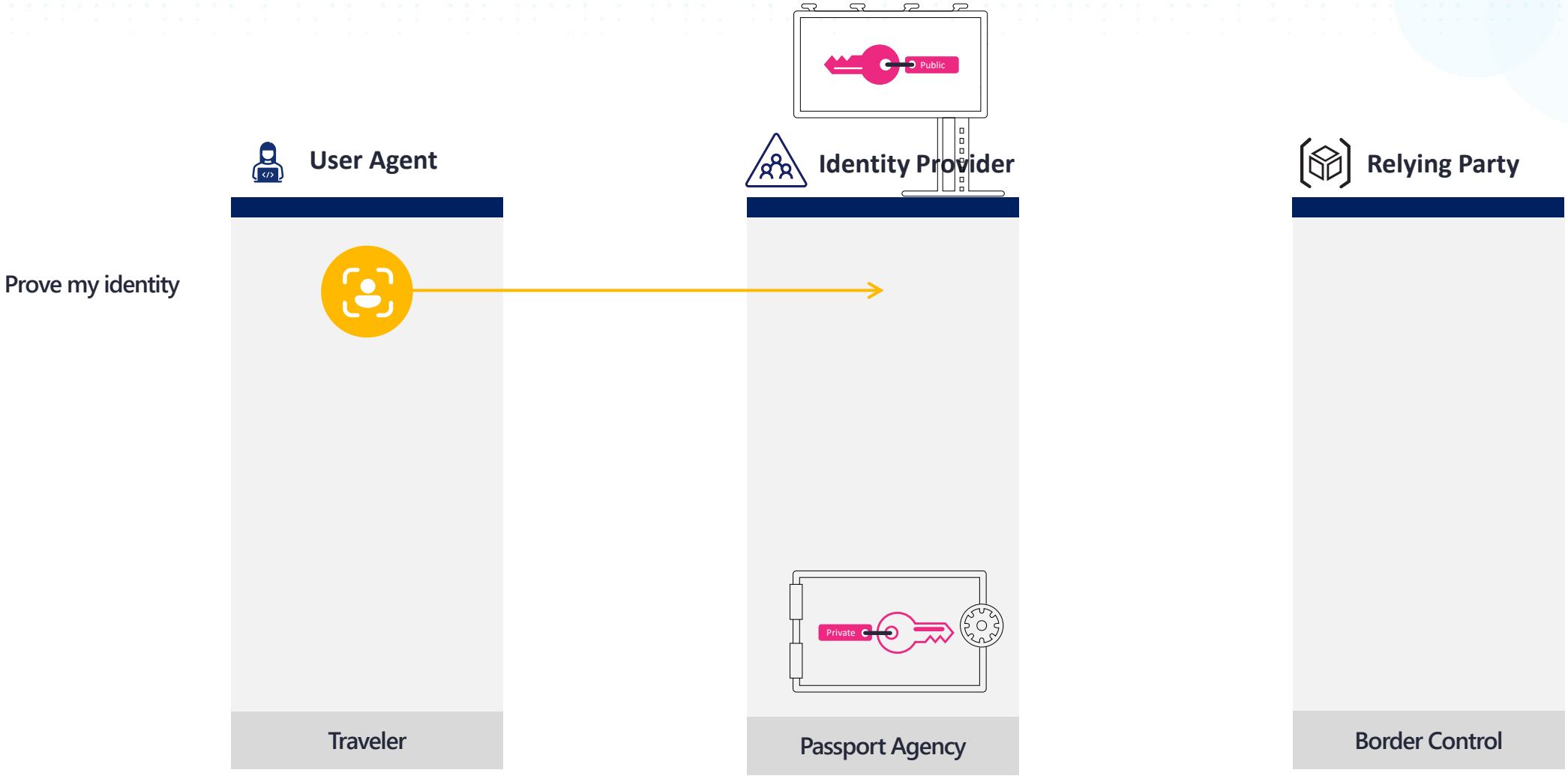
Proving authenticity in Single Sign-on



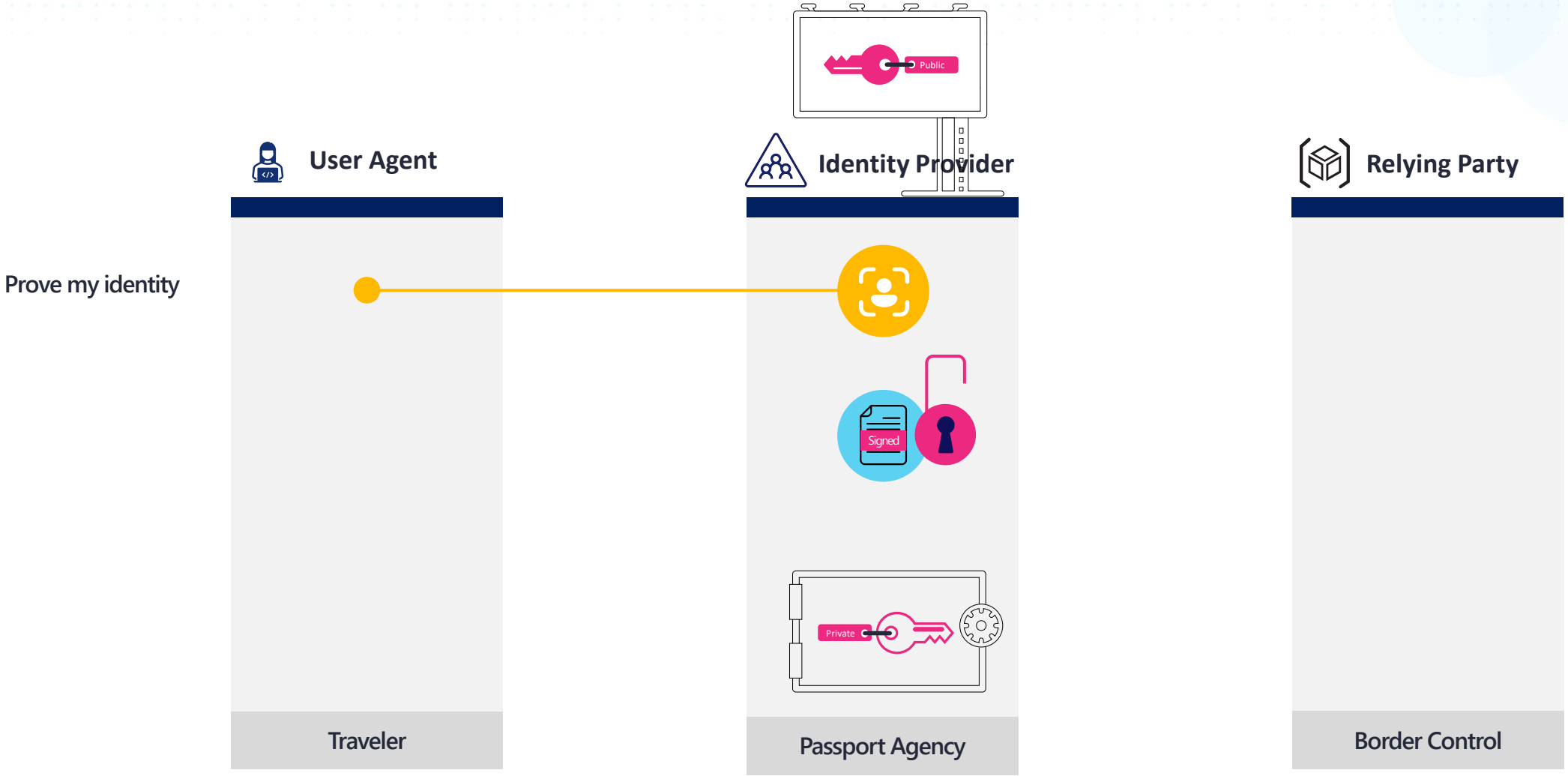
Proving authenticity in Single Sign-on



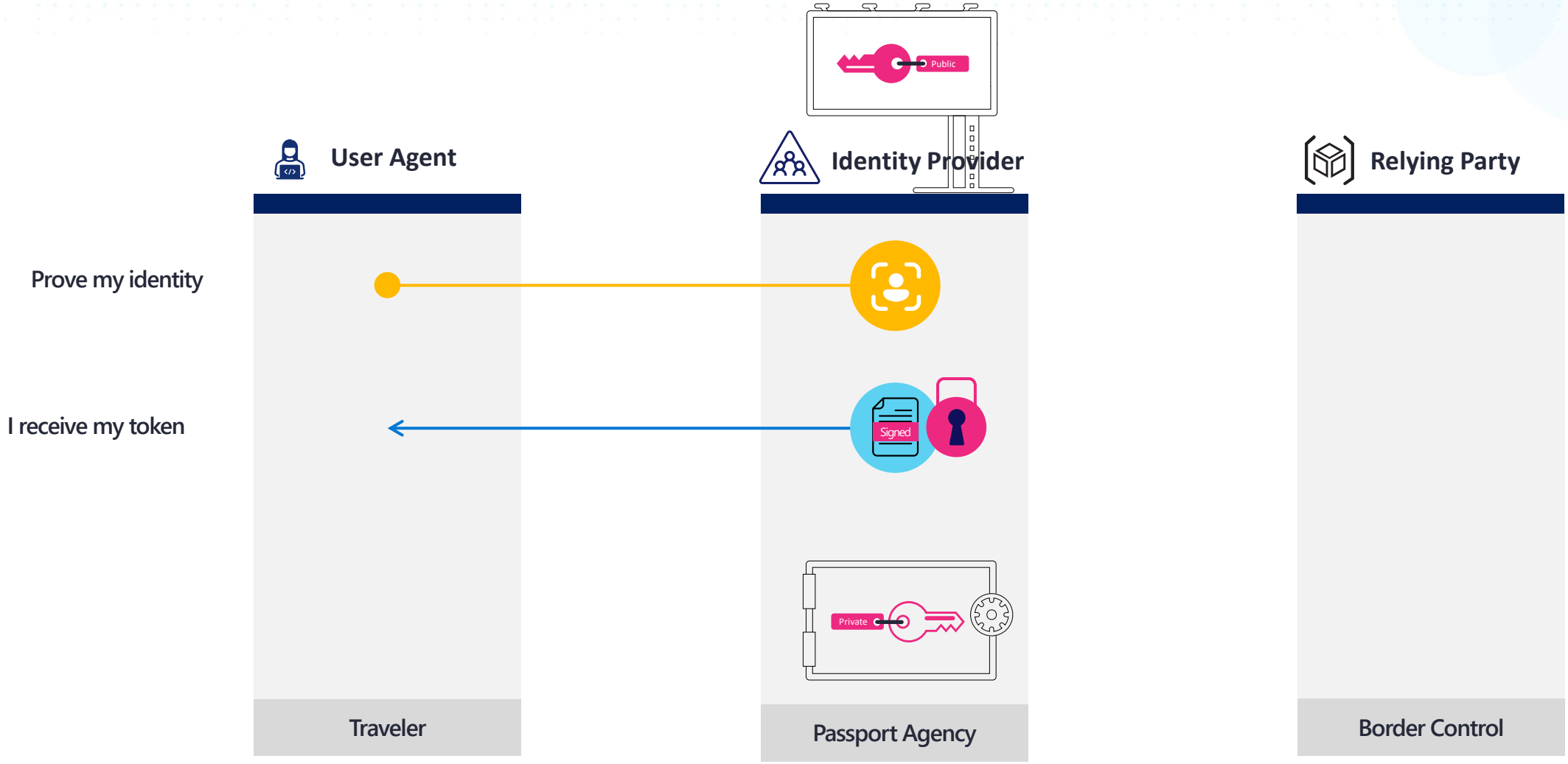
Proving authenticity in Single Sign-on



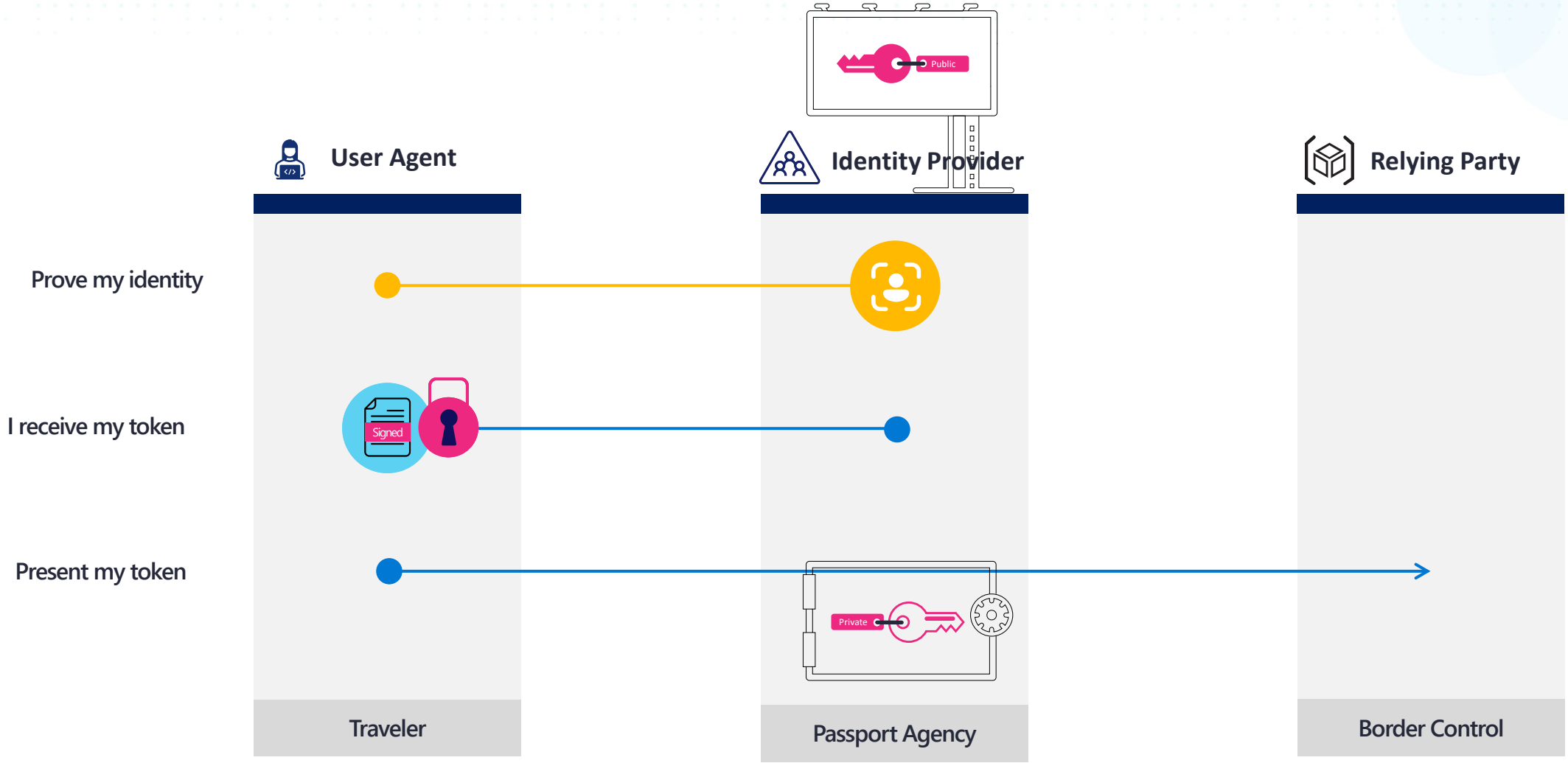
Proving authenticity in Single Sign-on



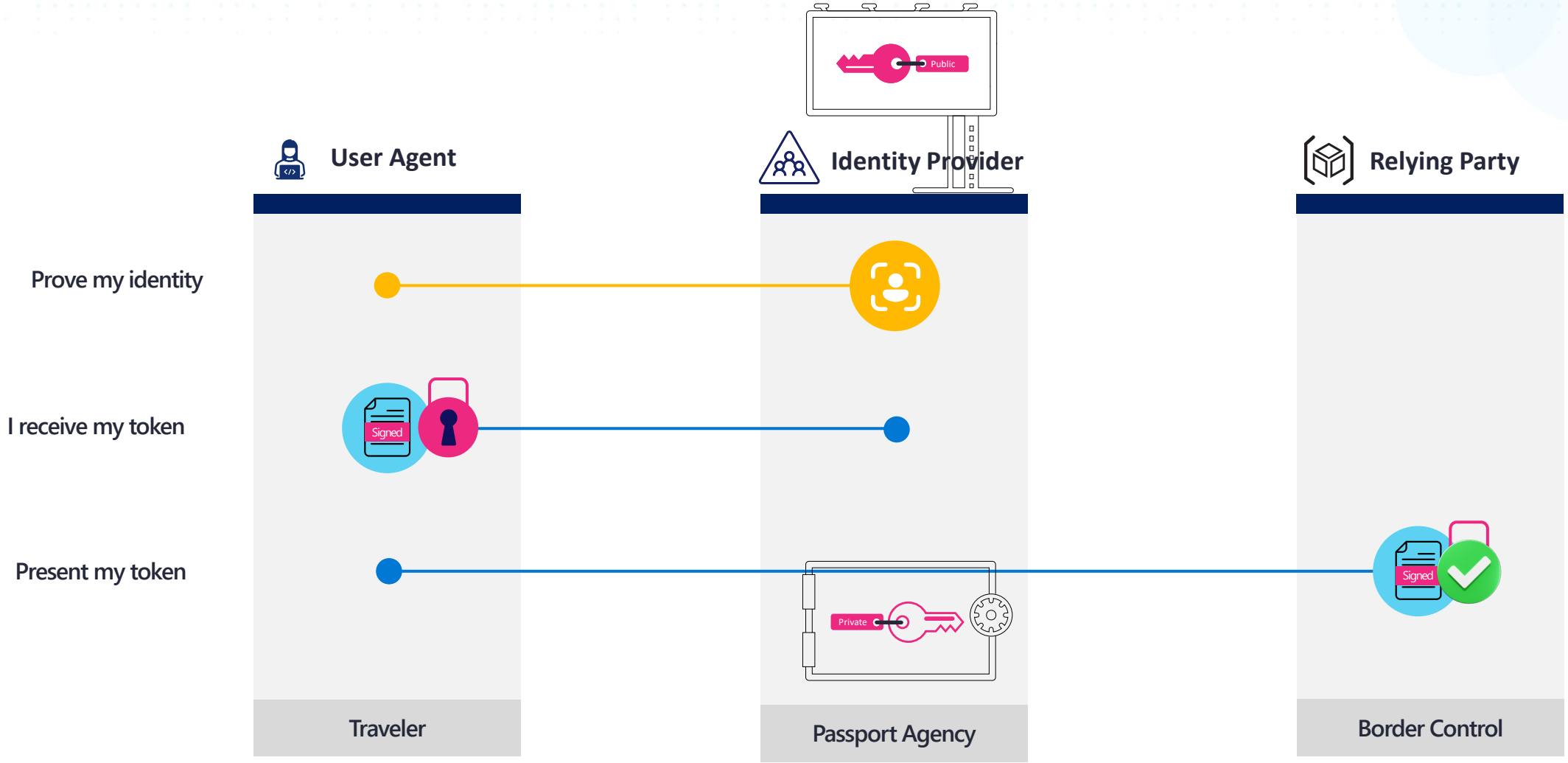
Proving authenticity in Single Sign-on



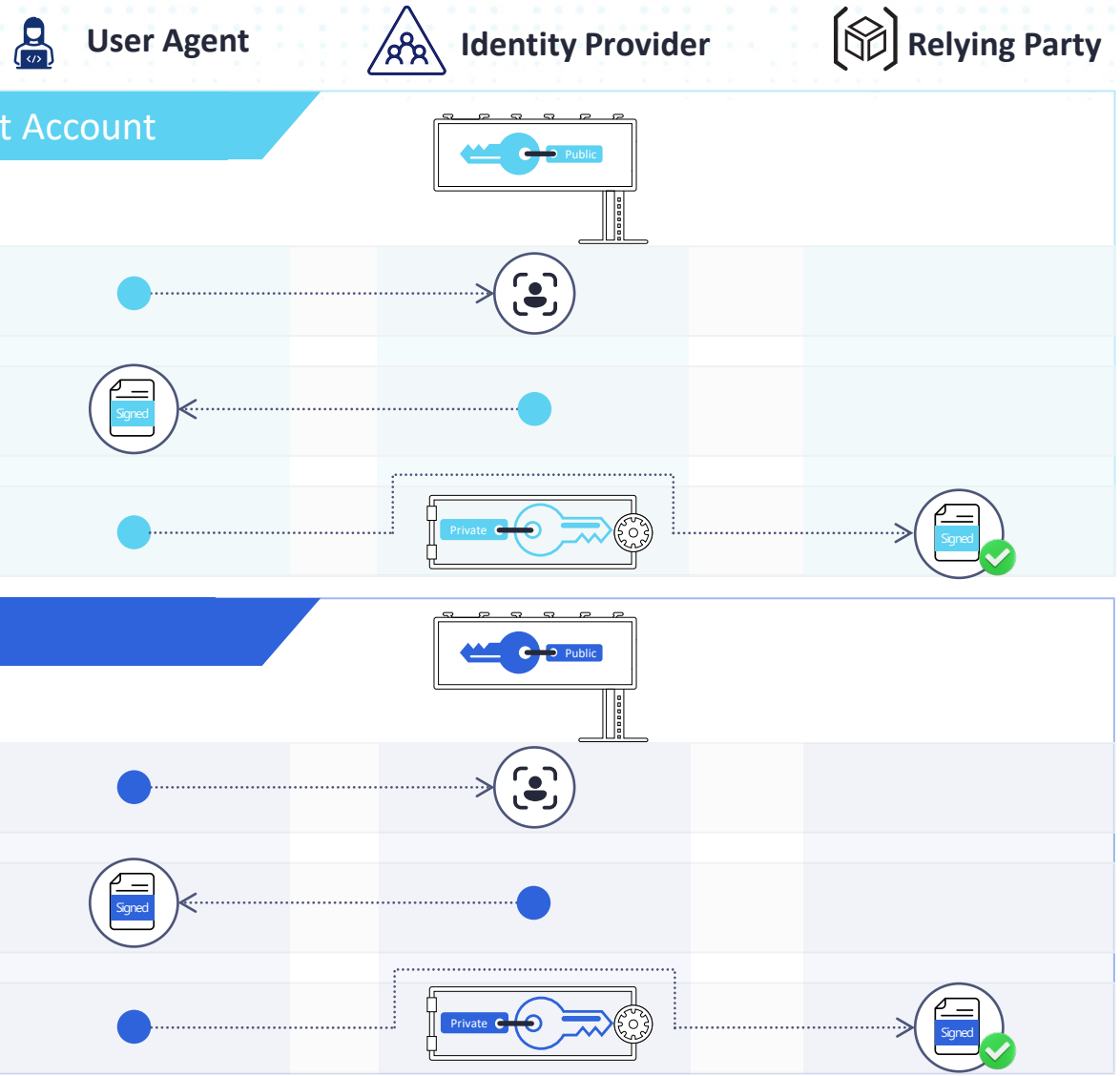
Proving authenticity in Single Sign-on



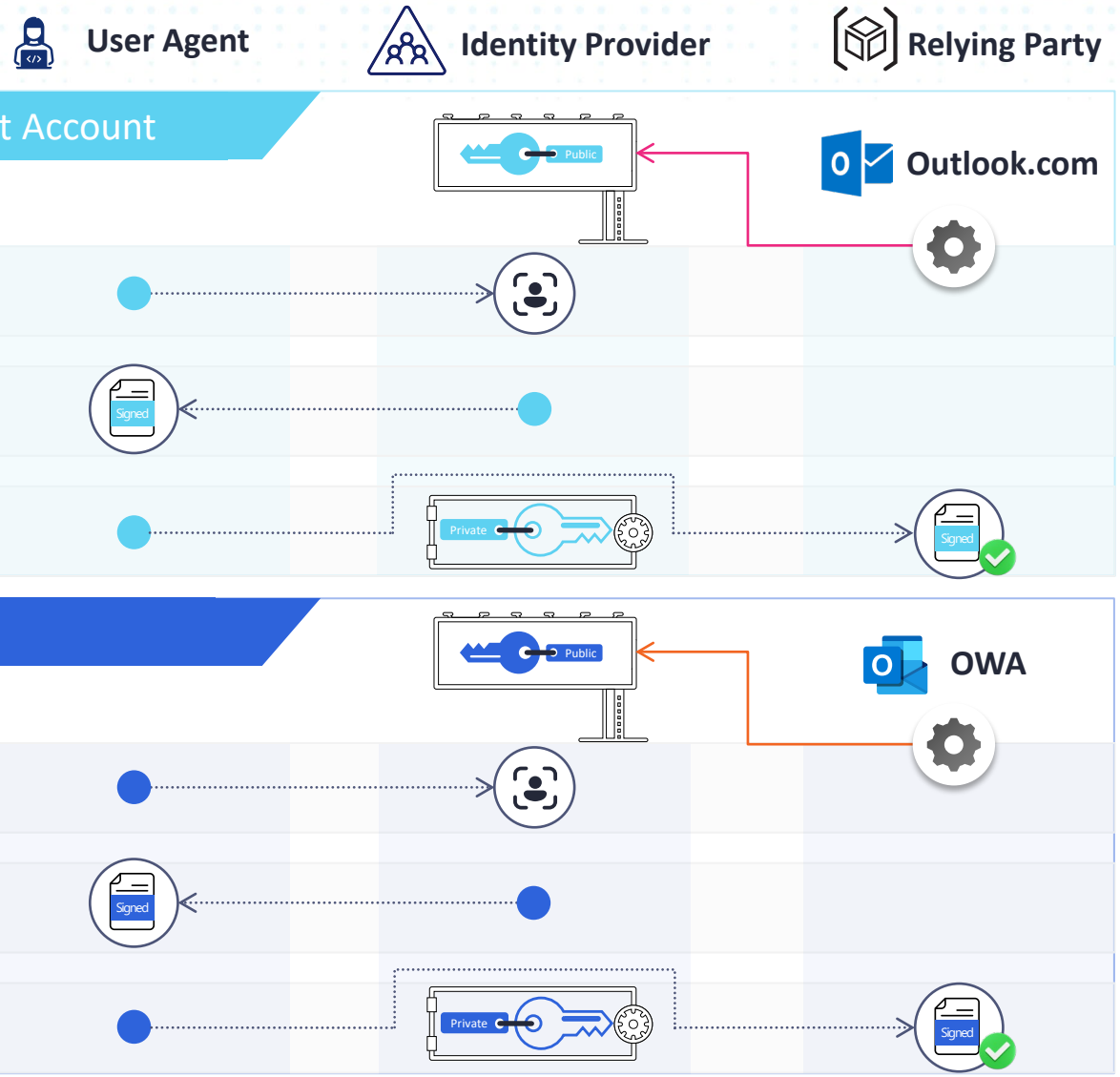
Proving authenticity in Single Sign-on



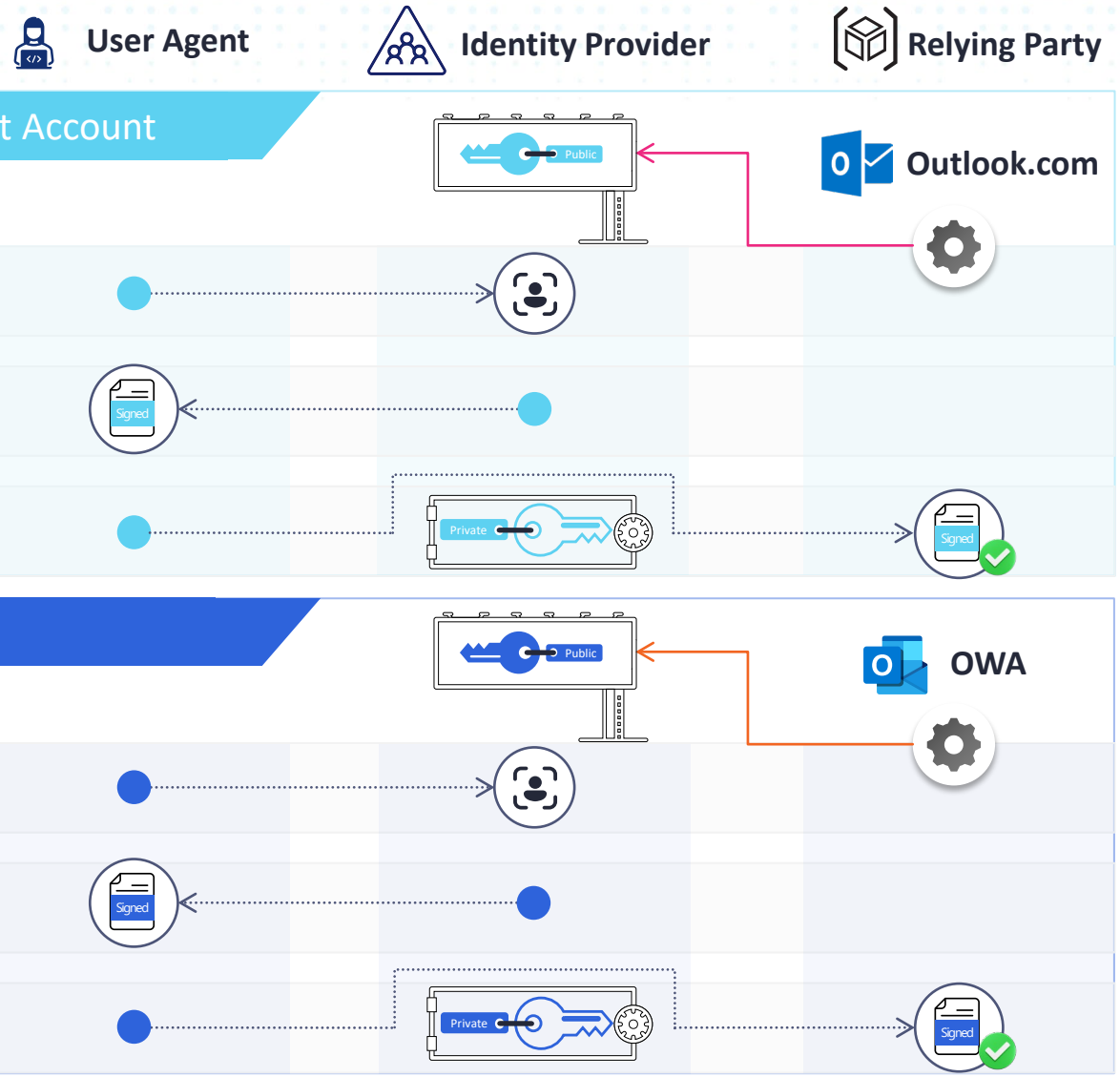
Single Sign-on at Microsoft in 2016

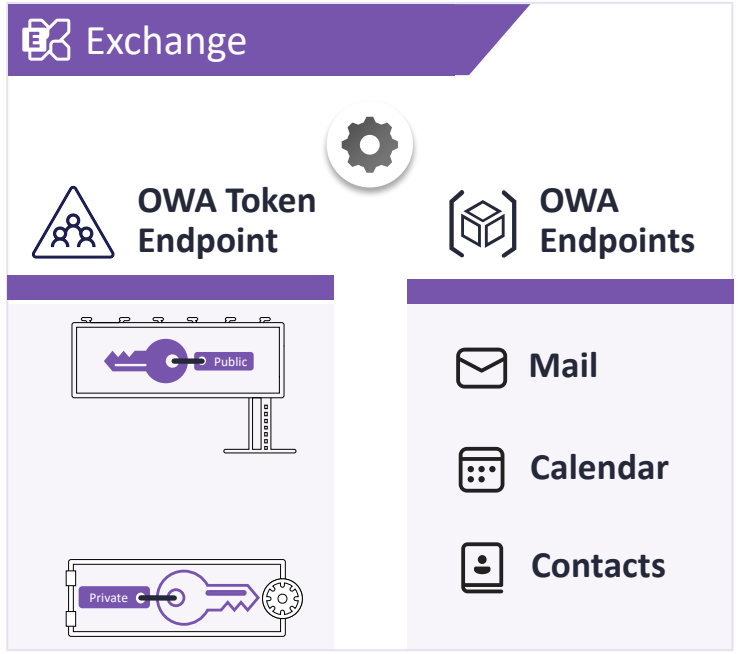


Single Sign-on at Microsoft in 2016

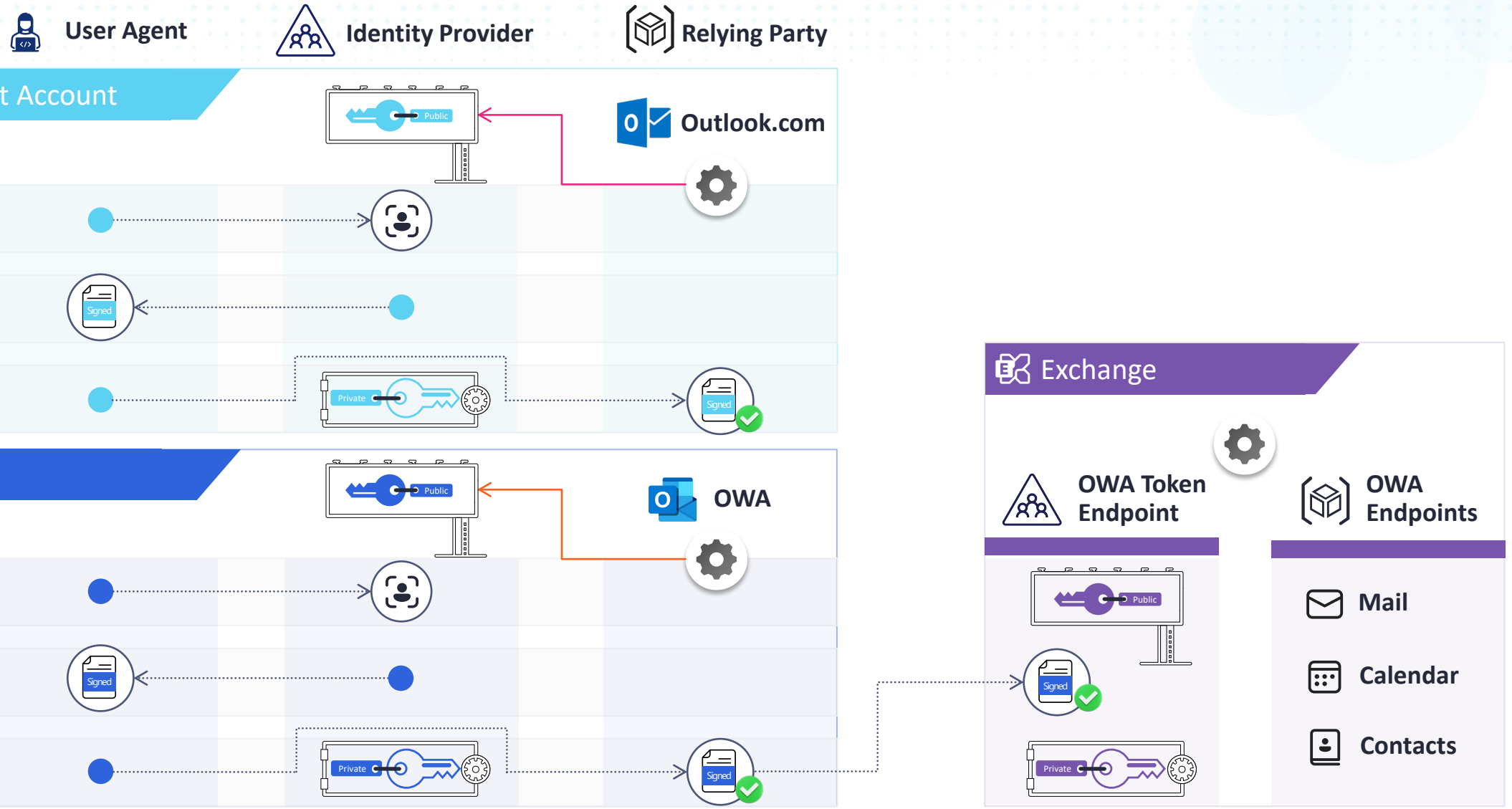


Single Sign-on at Microsoft in 2016

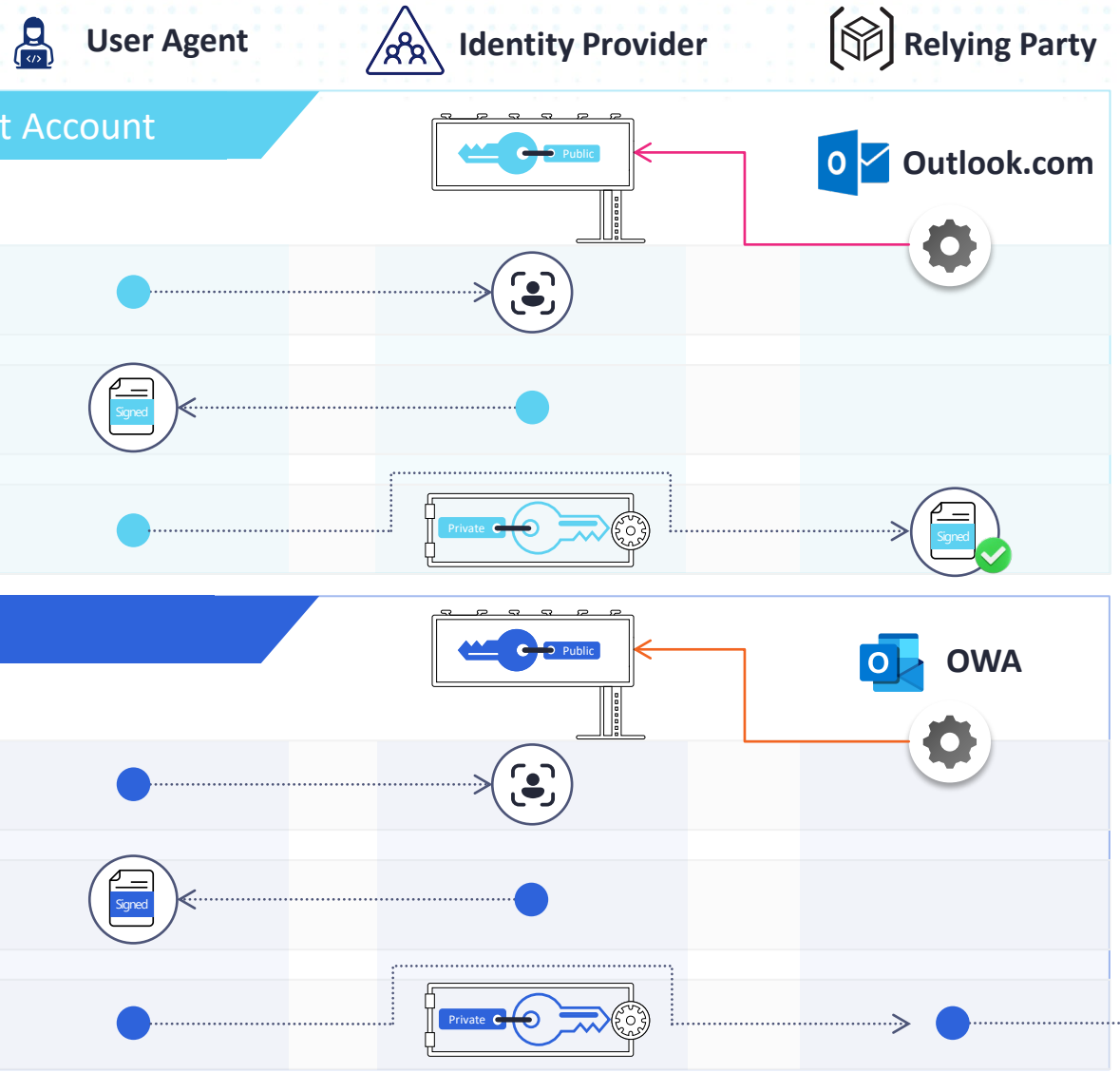




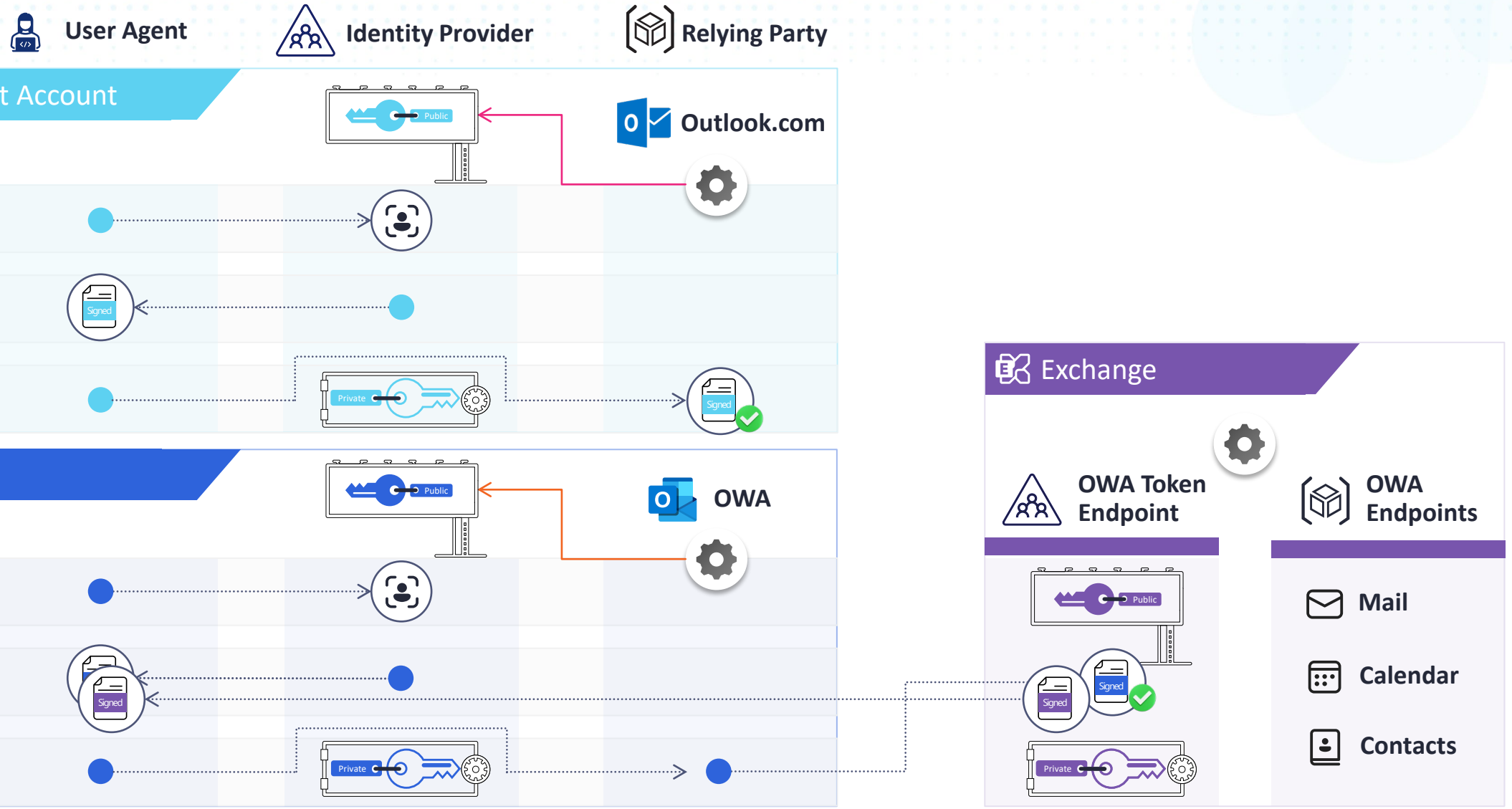
Single Sign-on at Microsoft in 2016



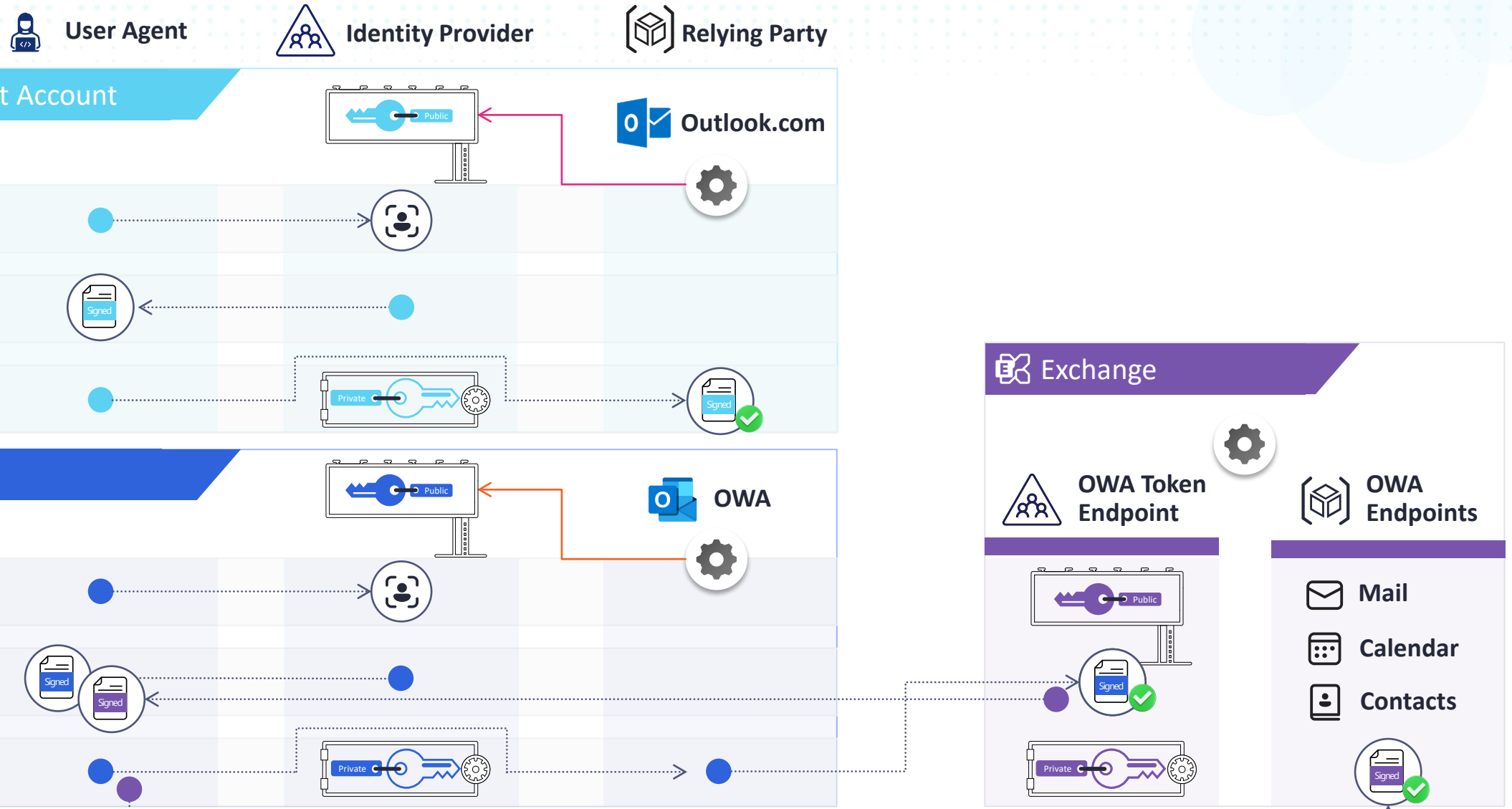
Single Sign-on at Microsoft in 2016



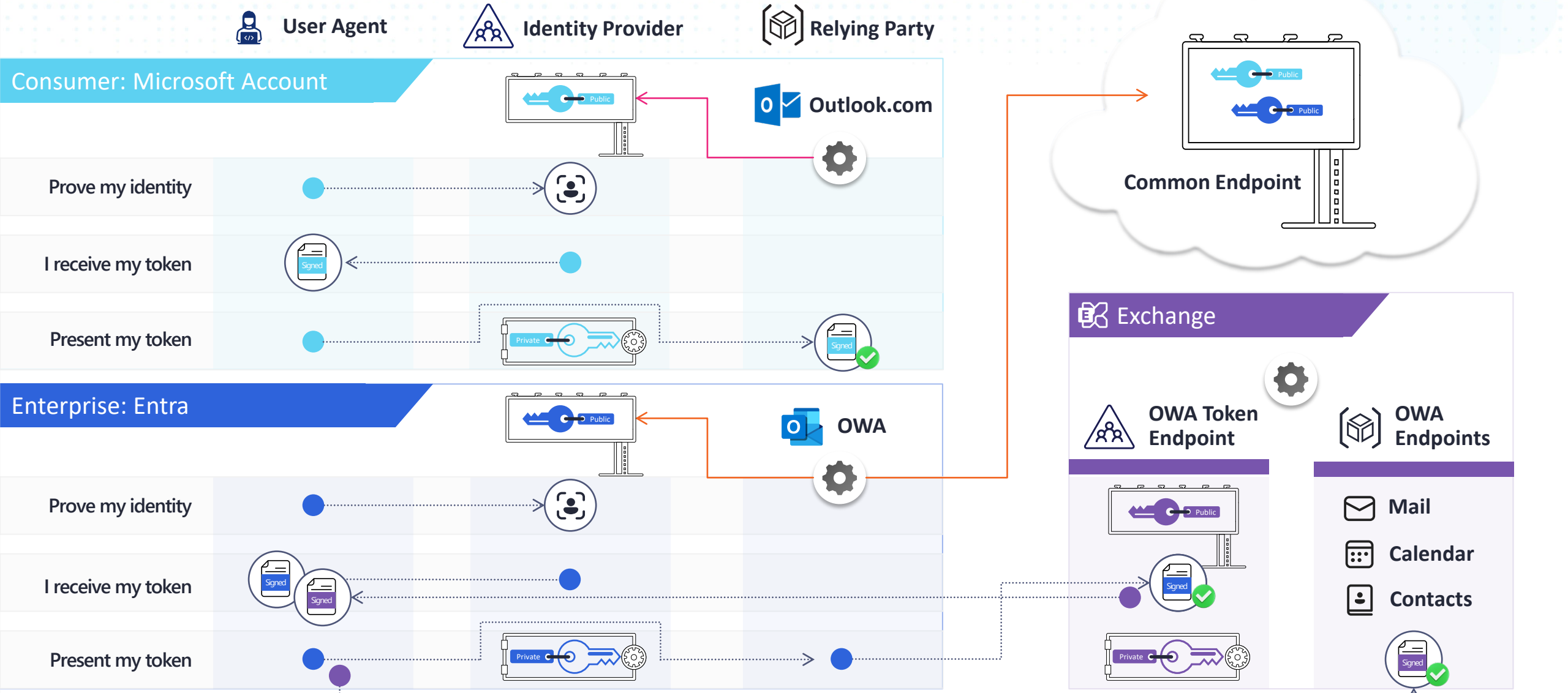
Single Sign-on at Microsoft in 2016



Single Sign-on at Microsoft in 2016

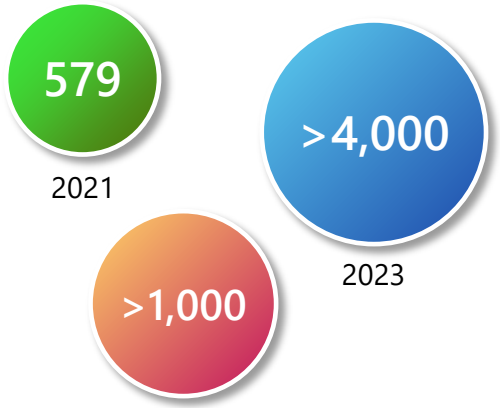


Single Sign-on at Microsoft 2018-2023



The odds are against defenders

Password attacks per second



Source: Microsoft

Organizations use an average of 80 security tools

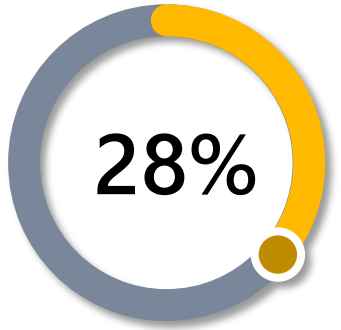
Source: Microsoft

Increase in phishing attacks, driven by attacker use of AI

Source: Zscaler

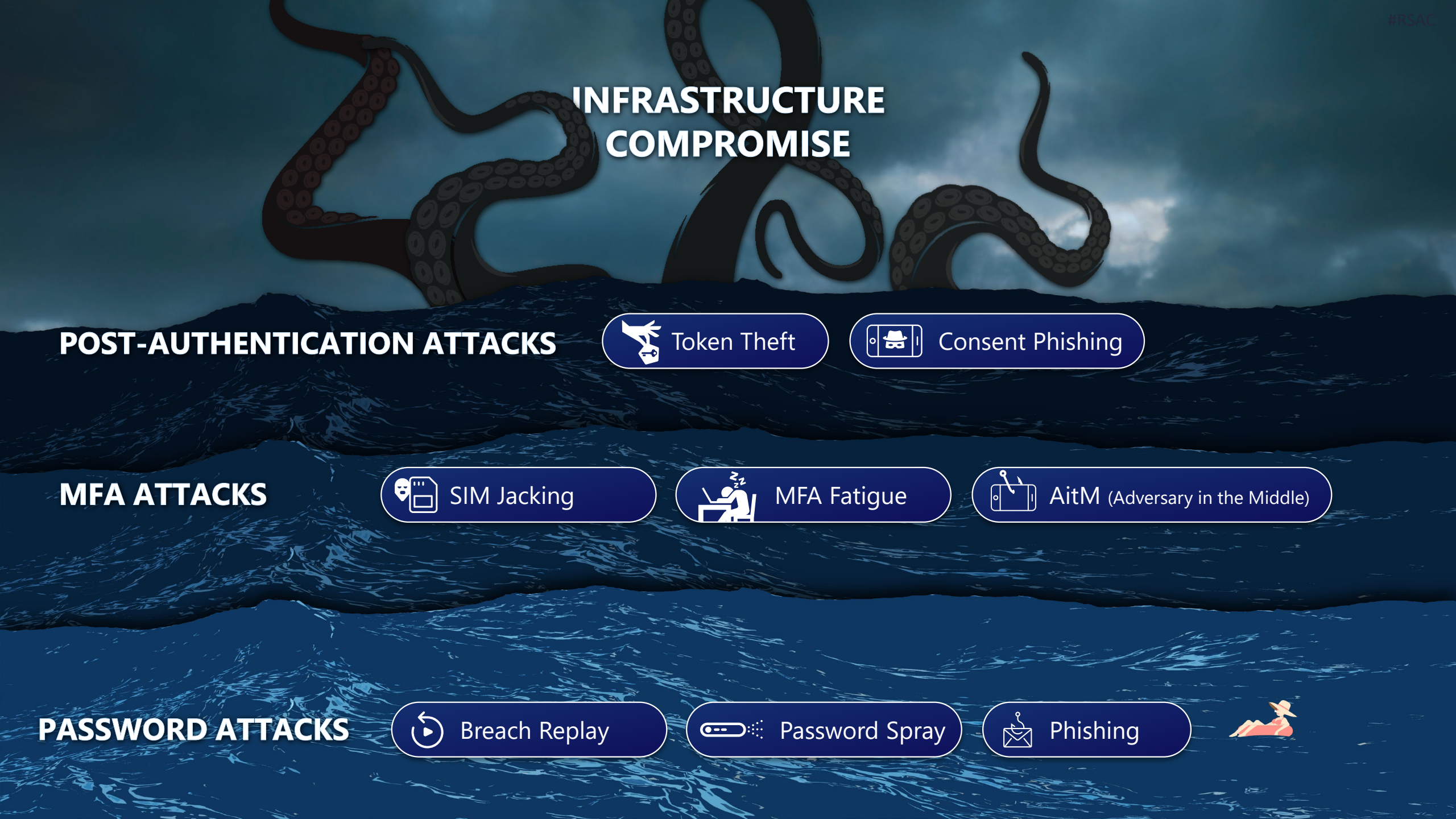
Open cybersecurity jobs globally

Source: (ISC)2



Business leaders concerned about data or IP loss due to improper use of AI

Source: IDC


INFRASTRUCTURE COMPROMISE
POST-AUTHENTICATION ATTACKS
Token Theft
Consent Phishing
MFA ATTACKS
SIM Jacking
MFA Fatigue
AitM (Adversary in the Middle)
PASSWORD ATTACKS
Breach Replay
Password Spray
Phishing

>2000

Nation State notifications a year

The pre-attack stage is set

- Identity systems for Consumer and Enterprise (and OWA)
- Common publishing endpoint and validation libraries
- Advanced ongoing nation state attacks on infrastructure

The players

Actor highlight:

Storm-0558

No known AKAs

Objectives

A distinct China-based threat actor group with geopolitical objectives focused on espionage and intelligence collection.

aka.ms/storm-0558

Primary Targets

Geography

- United States
- Western Europe
- Southeast Asia

Sectors

- Government agencies
- Diplomatic, economic, legislative governing bodies
- Media companies
- Educational institutions
- Think tanks
- Telecom equipment and service providers
- Individuals connected to Taiwan and Uyghur geopolitical interests
- IT Products and Services

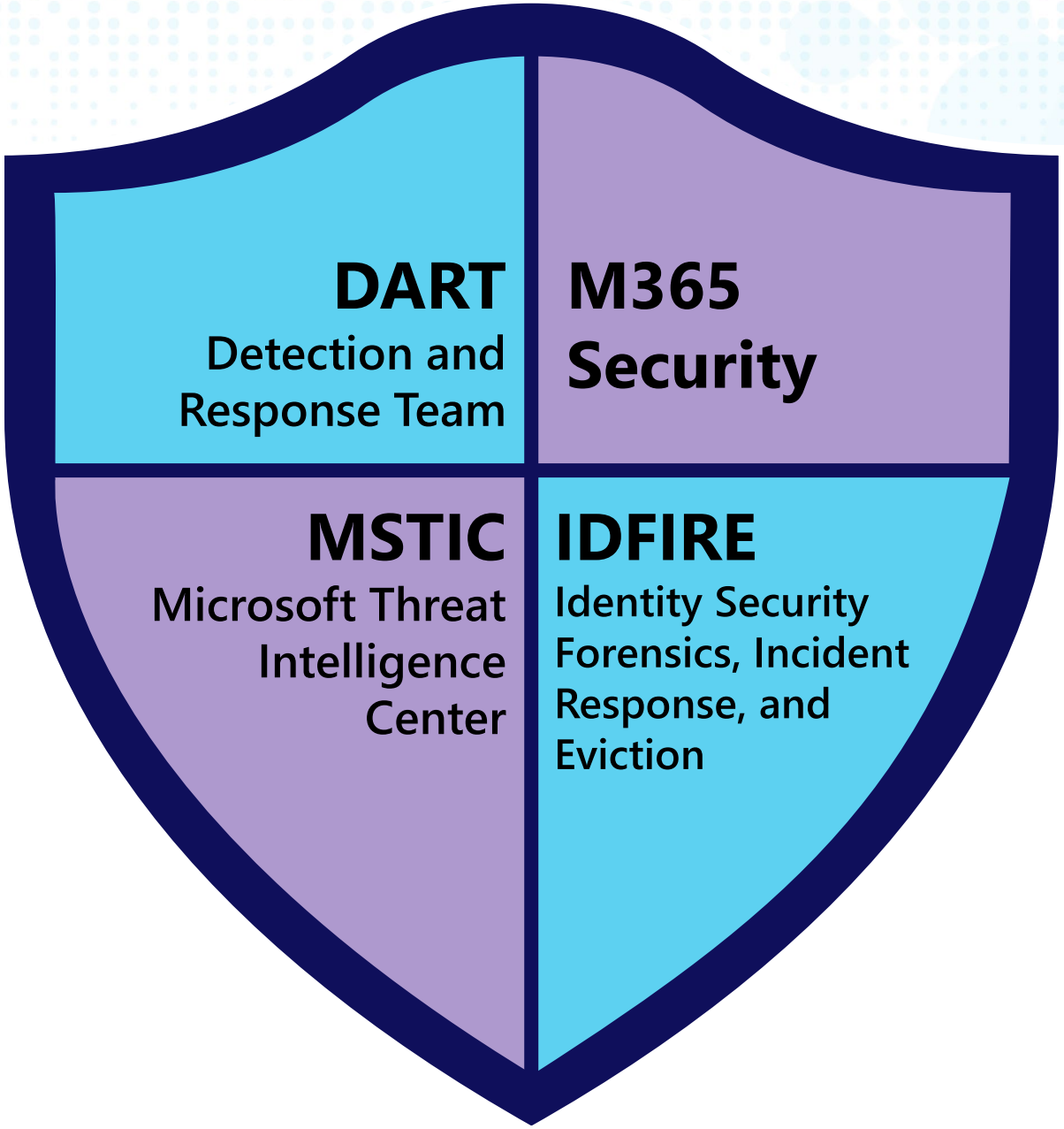
Microsoft Services

Entra

Exchange

Microsoft

Defenders building defenses




Department
Of
State
23rd Street Entrance
The Department of State is our nation's first executive department, established by Congress in 1789 to lead U.S. foreign policy.
The State Department protects and advances the American people's interests and values around the world, pursues economic opportunities abroad to drive prosperity at home, and assists Americans living or traveling overseas.
Since 1960, the Harry S Truman Building has served as the headquarters for State Department employees, who champion American diplomacy here and abroad. It is home to the Great Seal of the United States and the Diplomatic Reception Rooms, which contain one of the nation's finest collections of early American antiques.
For information on tours, please call (202) 647-3241. To learn more about the State Department, visit our website at http: www.state.gov.

The crime

June 15, 2023

- Customer detects anomalous mail access in analysis of logs.
- This specifically includes Exchange audit events for mail items accessed.

aka.ms/storm-0558

June 16, 2023

- Customer informs Microsoft Incident Response (DART) of attack.
- DART gathers forensic evidence from victim systems.
- DART shares findings with MSTIC for further investigation and attribution.

aka.ms/storm-0558

June 16, 2023

- MSTIC identifies the actor as Storm-0558.
- MSTIC identifies 21 additional targets.

actor intrusion techniques. Our profile was based on the following facets:

1. Hosts operating as part of this network present a JARM fingerprint consistent with SoftEther VPN: 06d06d07d06d06d06c42d42d000000cdb95e27fd8f9fee4a2bec829b889b8b.
2. Presented x509 certificate has expiration date of December 31, 2037.
3. Subject information within the x509 certificate does not contain "softether".

Over the course of the campaign, the IPs listed in the table below were used during the corresponding timeframes.

IP address	First seen	Last seen	Description
51.89.156[.]153	3/9/2023	7/10/2023	SoftEther proxy
176.31.90[.]129	3/28/2023	6/29/2023	SoftEther proxy
137.74.181[.]100	3/31/2023	7/11/2023	SoftEther proxy

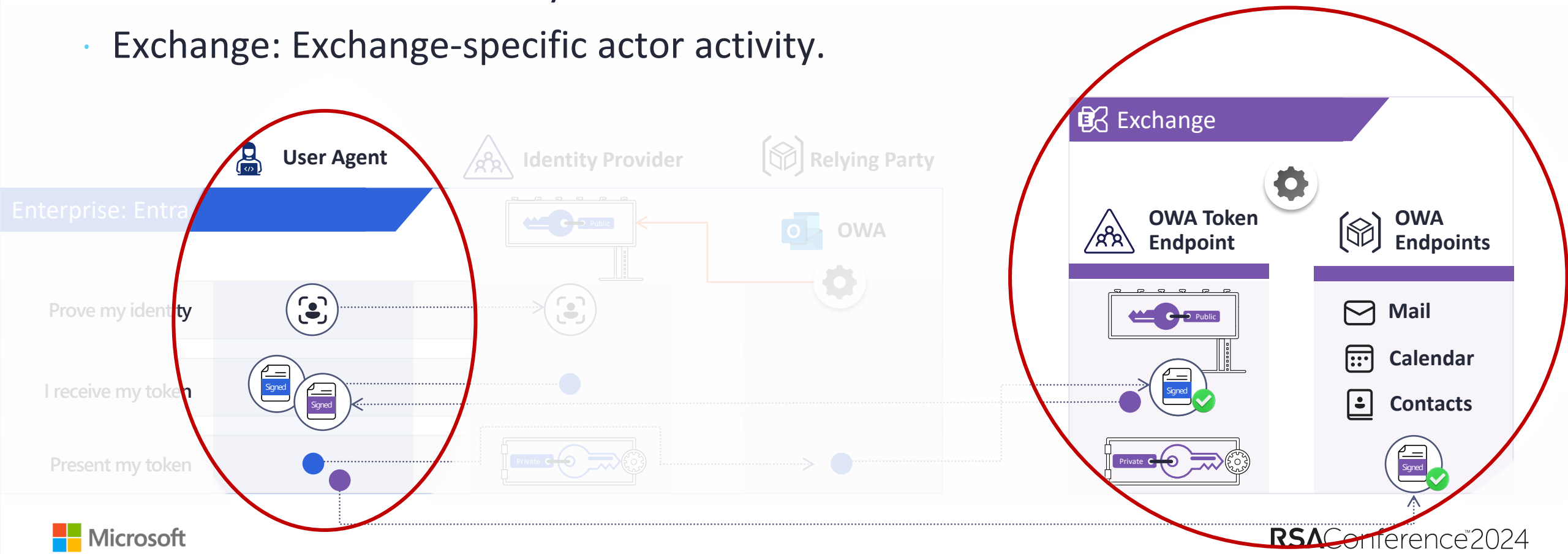
IP address	First seen	Last seen	Description
195.26.87[.]219	5/15/2023	6/25/2023	Token web panel
185.236.228[.]183	5/24/2023	6/11/2023	Token web panel
85.239.63[.]160	6/7/2023	6/11/2023	Token web panel

aka.ms/storm-0558

June 16-26, 2023

Investigation focusing on:

- DART: How customer was compromised.
- MSTIC: Other actor activity.
- Exchange: Exchange-specific actor activity.



June 25, 2023

MSTIC finds an unsecured actor server while investigating actor infrastructure and captures source code.

```
def Check_Status():
    #global Bearer_AT
    while True:
        RequestURL = "https://outlook.office.com/owa/service.svc?action=GetAccessTokenforResource&UA=0&app=Mail&n=12"
        headers = {
            "authority": "outlook.office.com",
            "accept": "*/*",
            "accept-language": "en-US,en;q=0.9",
            "accept-encoding": "gzip, deflate, br",
            "action": "GetAccessTokenforResource",
            "content-type": "application/json; charset=utf-8",
            "origin": "https://outlook.office.com",
            "Authorization": dic["token"],
            "sec-ch-ua-platform": "Windows",
            "sec-ch-ua-mobile": "?0",
            "user-agent": "Client=REST;Client=RESTSystem;;",
            # "x-owa-canary":
            "x-owa-urlpostdata": "%7B%22__type%22%3A%22TokenRequest%3A%23Exchange%22%2C%22Resource%22%3A%22https%3A%2F%2Foutlook.office.com%22%7D",
            "x-req-source": "Mail",

        }

        message = requests.post(url=RequestURL, headers=headers).json()
        #print(message)
        Response_AT = "Bearer " + message["AccessToken"]
        Expiration_Count_Down = message["ExpiresIn"]
        Expiration_Accurate_Time = message["AccessTokenExpiry"]

        if Response_AT == dic["token"]:
            print("AT unchanged \n")
            print("AT will expire at " + str(Expiration_Accurate_Time))
            print("AT will expire in " + str(Expiration_Count_Down) + " seconds")
            time.sleep(Expiration_Count_Down + 5)

        else:
            print("AT has refreshed, " + "New AT is " + Response_AT + "\n")
            print("Start to Log...")
            #print(Response_AT + "\n")
            Log(Response_AT, Expiration_Accurate_Time)
            dic["token"] = Response_AT
            # return Init_AT
            print("AT will expire in " + str(Expiration_Count_Down) + "seconds")
            time.sleep(Expiration_Count_Down + 5)
```

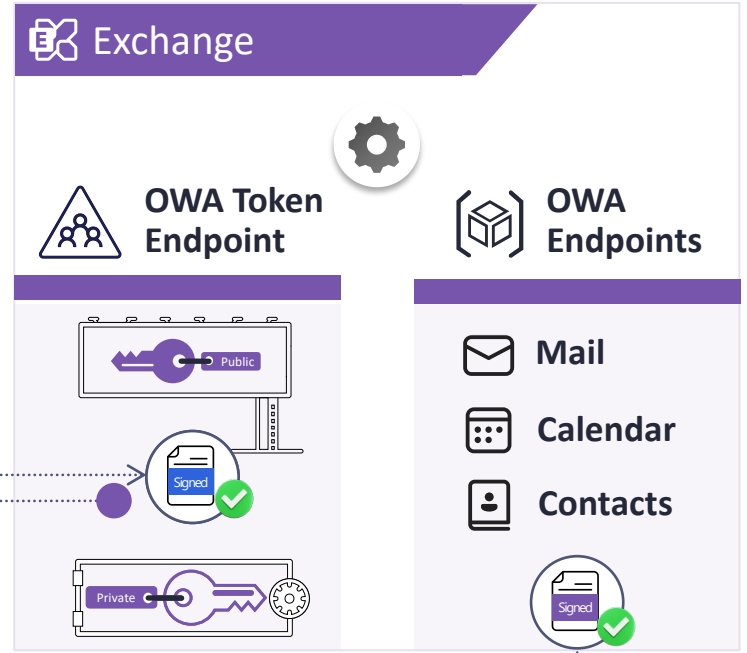
» aka.ms/storm-0558

June 26, 2023

Determined actor was abusing endpoint **`GetAccessTokensForResource`** to bypass OWA token refresh.

OWA team takes immediate action:

> "On June 26, OWA stopped accepting tokens issued from **`GetAccessTokensForResource`** for renewal, which mitigated the token renewal being abused."



aka.ms/storm-0558

June 27, 2023

M365 Security suspects tokens may be forged, engages IDFIRE.

IDFIRE finds evidence token may be forged:

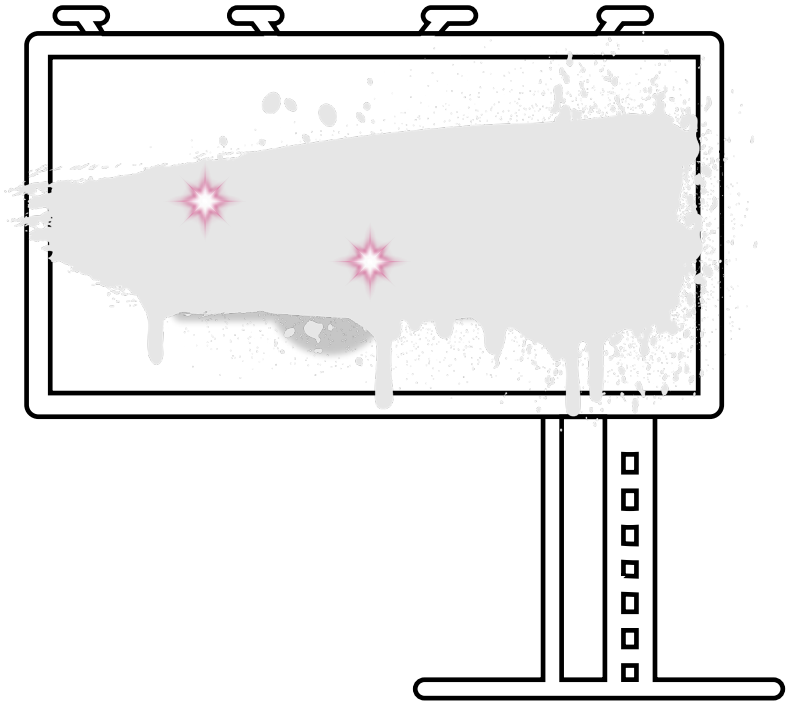
- Format is subtly wrong.
- Signed with an inactive consumer key.
- Not found in issuance logs.

June 27, 2023

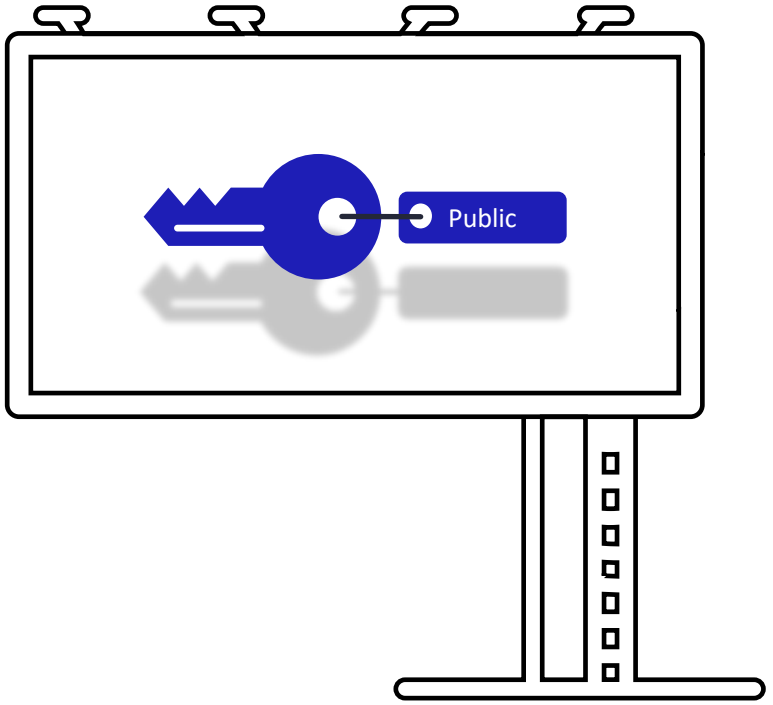

FIRE ALARM
PUSH
PULL DOWN
STANDARDIZED SECURITY
INCIDENT RESPONSE
PROTOCOL

June 27, 2023

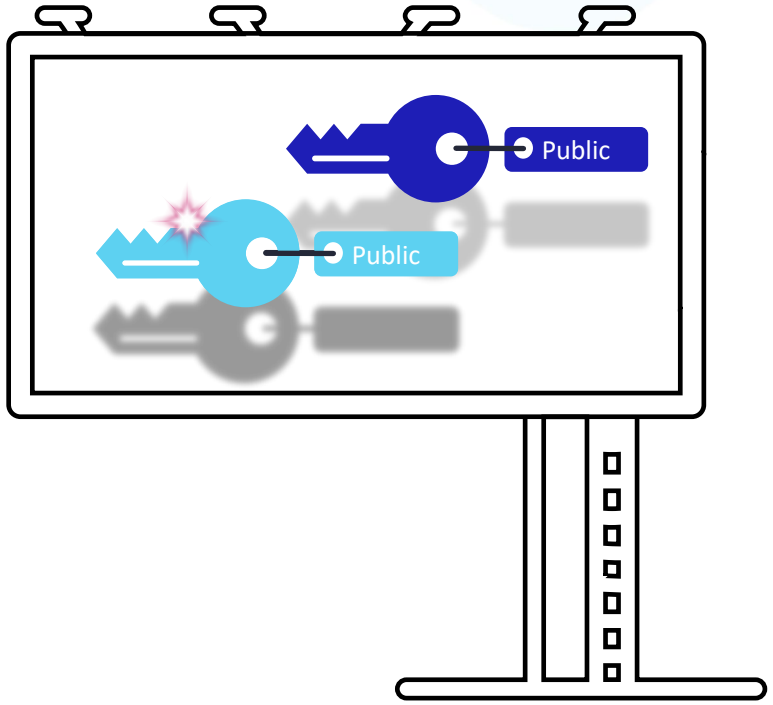
Consumer



Enterprise



Common

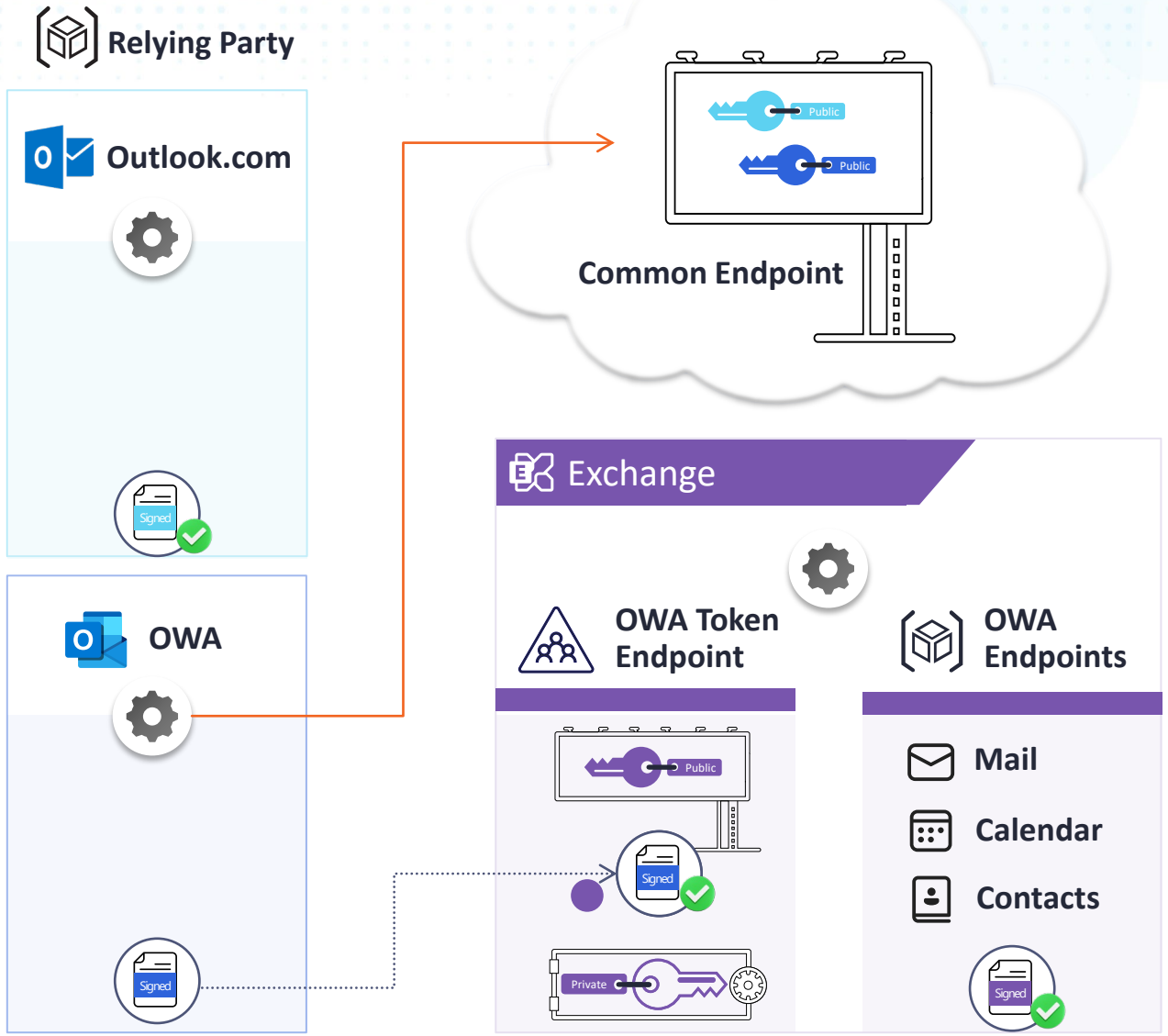


June 27, 2023

Identified validation issue.

"...to improve security of token validation ... we released defense-in-depth changes to the Microsoft.IdentityModel and Microsoft.Identity.Web libraries."

aka.ms/storm-0558



Beginning June 27, 2023

IDFIRE analyzes relying party logs for Microsoft services

22 organizations affected
+ 502 consumer accounts
Users notified

No other evidence of use of key

June 27, 2023

OWA explicitly rejects all tokens with the offending key's thumbprint.

Monitoring confirms actor activity in OWA stops at this point.

MSTIC monitoring also indicates that the actor has shifted back to phishing attacks

June 29, 2023

Public key removal propagated to all services worldwide.

The public key component of the impacted private key is no longer advertised anywhere – revocation complete.

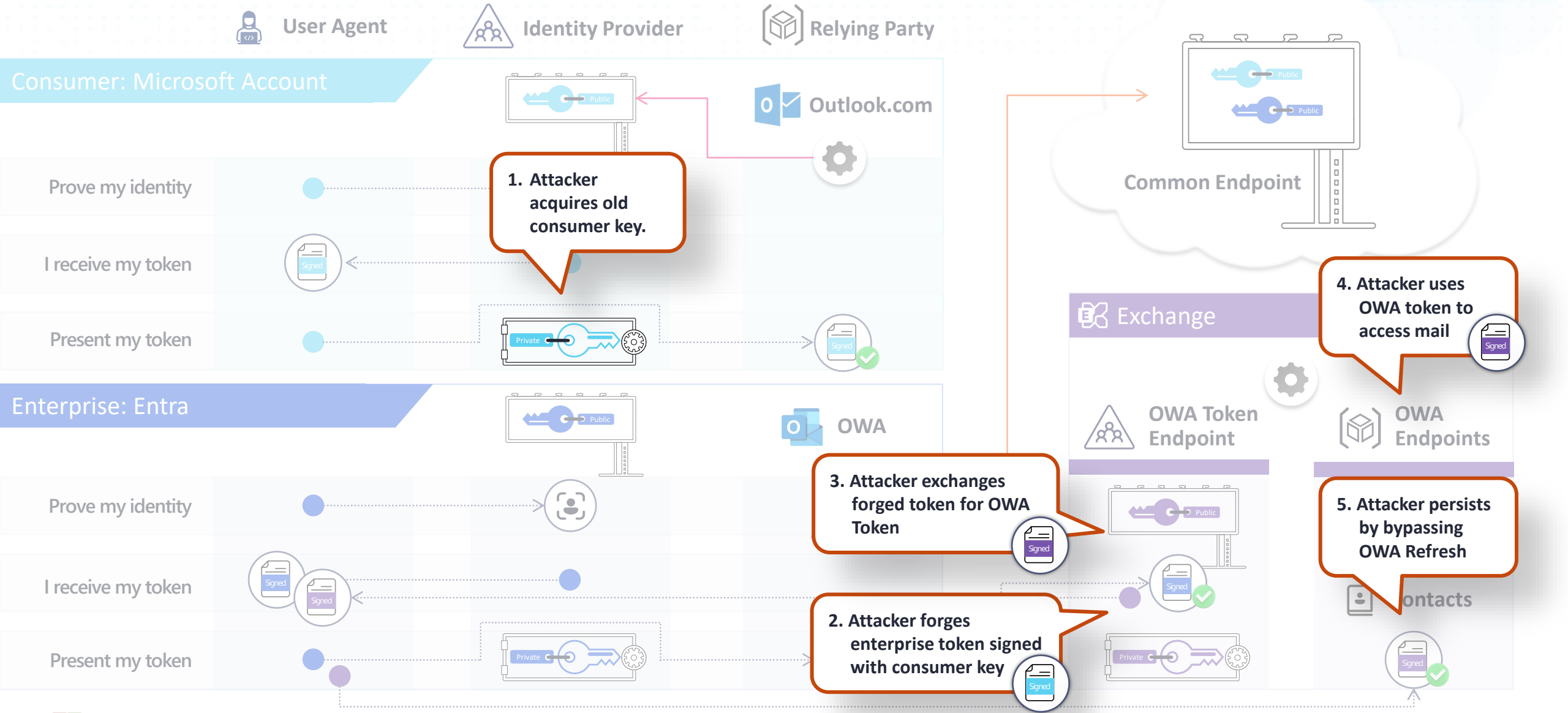
July 3, 2023

Refresh of any consumer tokens created with the offending private key blocked.

Monitoring confirms all actor activity in Outlook.com stopped at this point.

aka.ms/storm-0558

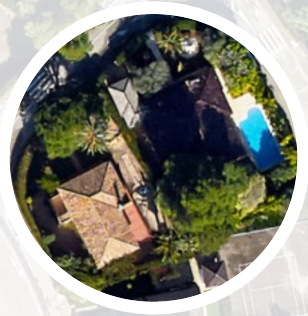
Full attack mechanics



Hypothetical impact

Actual impact

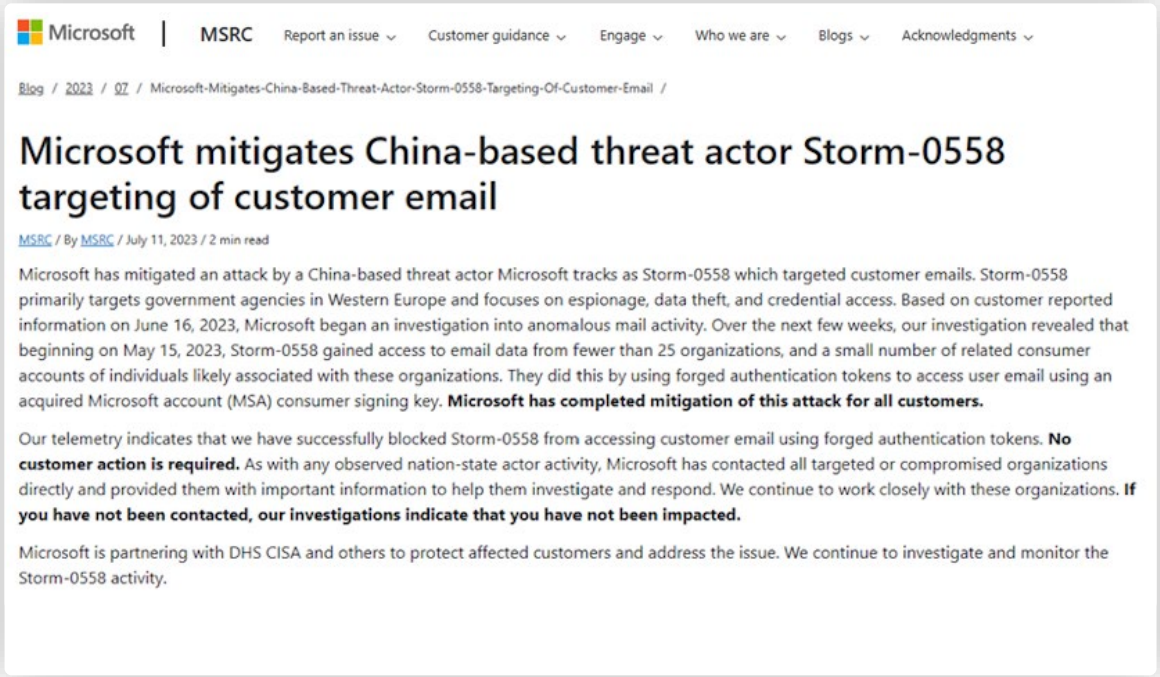
Mail for **22** organizations and **502** consumers



- Monitoring of actor VPN traffic
- Exhaustive review of logs
- Capture of actor source code
- Correlation to prior actor patterns
- Change in actor pattern after keys were rolled

July 11, 2023

Two blogs published related to activity



Microsoft | MSRC Report an issue Customer guidance Engage Who we are Blogs Acknowledgments

Blog / 2023 / 07 / Microsoft-Mitigates-China-Based-Threat-Actor-Storm-0558-Targeting-Of-Customer-Email /

Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 2 min read

Microsoft has mitigated an attack by a China-based threat actor Microsoft tracks as Storm-0558 which targeted customer emails. Storm-0558 primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access. Based on customer reported information on June 16, 2023, Microsoft began an investigation into anomalous mail activity. Over the next few weeks, our investigation revealed that beginning on May 15, 2023, Storm-0558 gained access to email data from fewer than 25 organizations, and a small number of related consumer accounts of individuals likely associated with these organizations. They did this by using forged authentication tokens to access user email using an acquired Microsoft account (MSA) consumer signing key. **Microsoft has completed mitigation of this attack for all customers.**

Our telemetry indicates that we have successfully blocked Storm-0558 from accessing customer email using forged authentication tokens. **No customer action is required.** As with any observed nation-state actor activity, Microsoft has contacted all targeted or compromised organizations directly and provided them with important information to help them investigate and respond. We continue to work closely with these organizations. **If you have not been contacted, our investigations indicate that you have not been impacted.**

Microsoft is partnering with DHS CISA and others to protect affected customers and address the issue. We continue to investigate and monitor the Storm-0558 activity.

Microsoft | Microsoft On the Issues Our Company News and Stories Topics Cloud Principles Press Tools

Mitigation for China-based threat actor activity

Jul 11, 2023 | Charlie Bell - Executive Vice President, Microsoft Security

Microsoft and others in the industry have called for transparency when it comes to cyber incidents so that we can learn and get better. As we've stated previously, we cannot ignore the exponential rise and frequency of sophisticated attacks. The growing challenges we face only reinforce our commitment to greater information sharing and industry partnership.

Today, we are publishing details of activity by a China-based actor Microsoft is tracking as Storm-0558 that gained access to email accounts affecting approximately 25 organizations including government agencies as well as related consumer accounts of individuals likely associated with these organizations. We have been working with the impacted customers and notifying them prior to going public with further details. At this stage – and in coordination with customers – we are sharing the details of the incident and threat actor to benefit the industry.

Cyberattacks continue to rise in sophistication and frequency

» aka.ms/storm-0558

ongoing
The investigation

How did this happen?

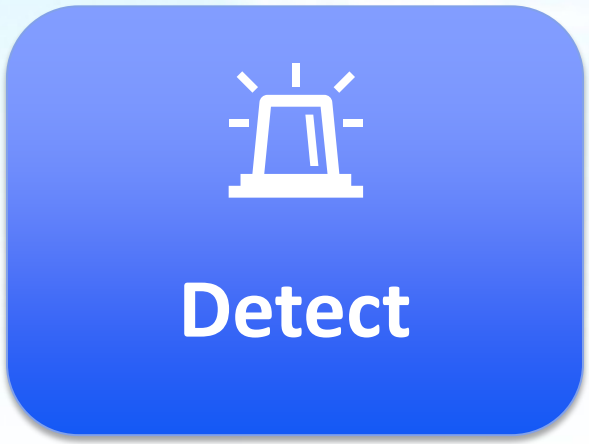
Operator error?

Insider attack?

Was it quantum?

Crash handling?

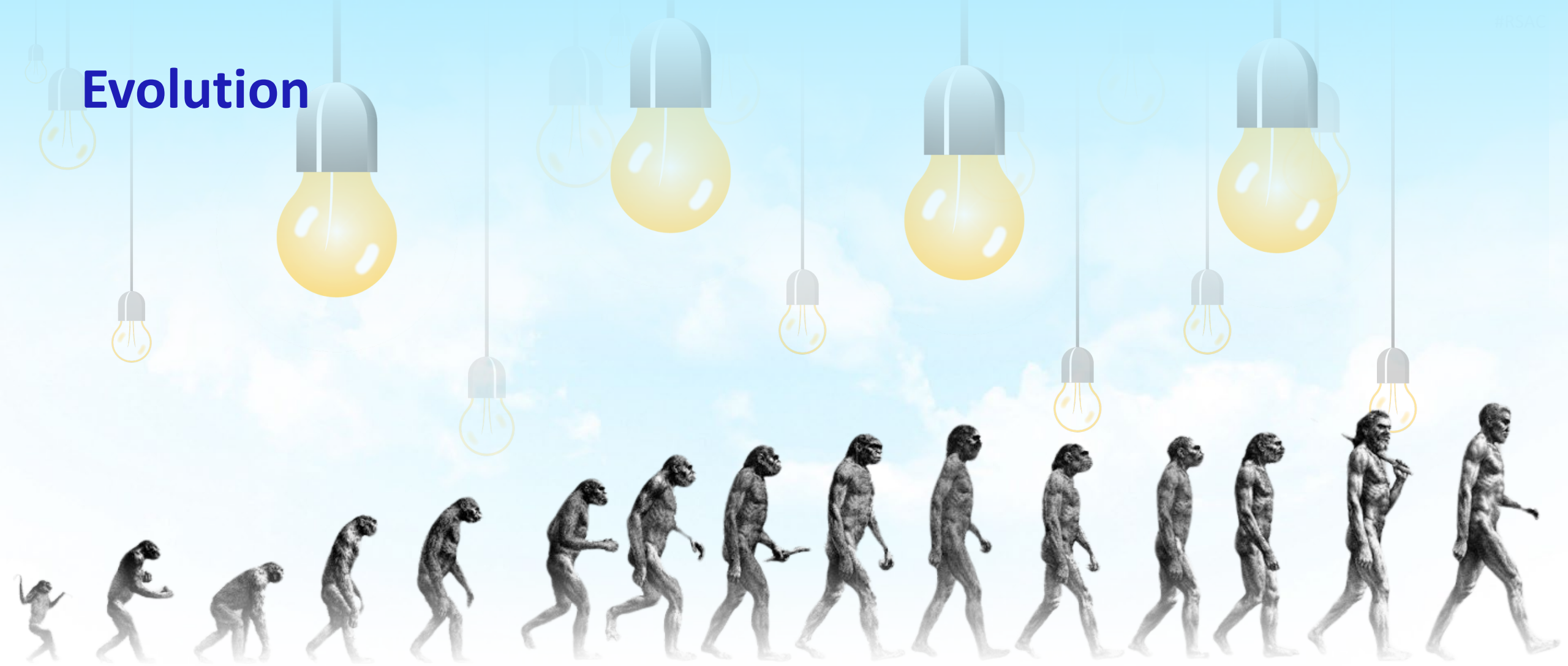
The workstreams



The workstreams

Insights and improvements

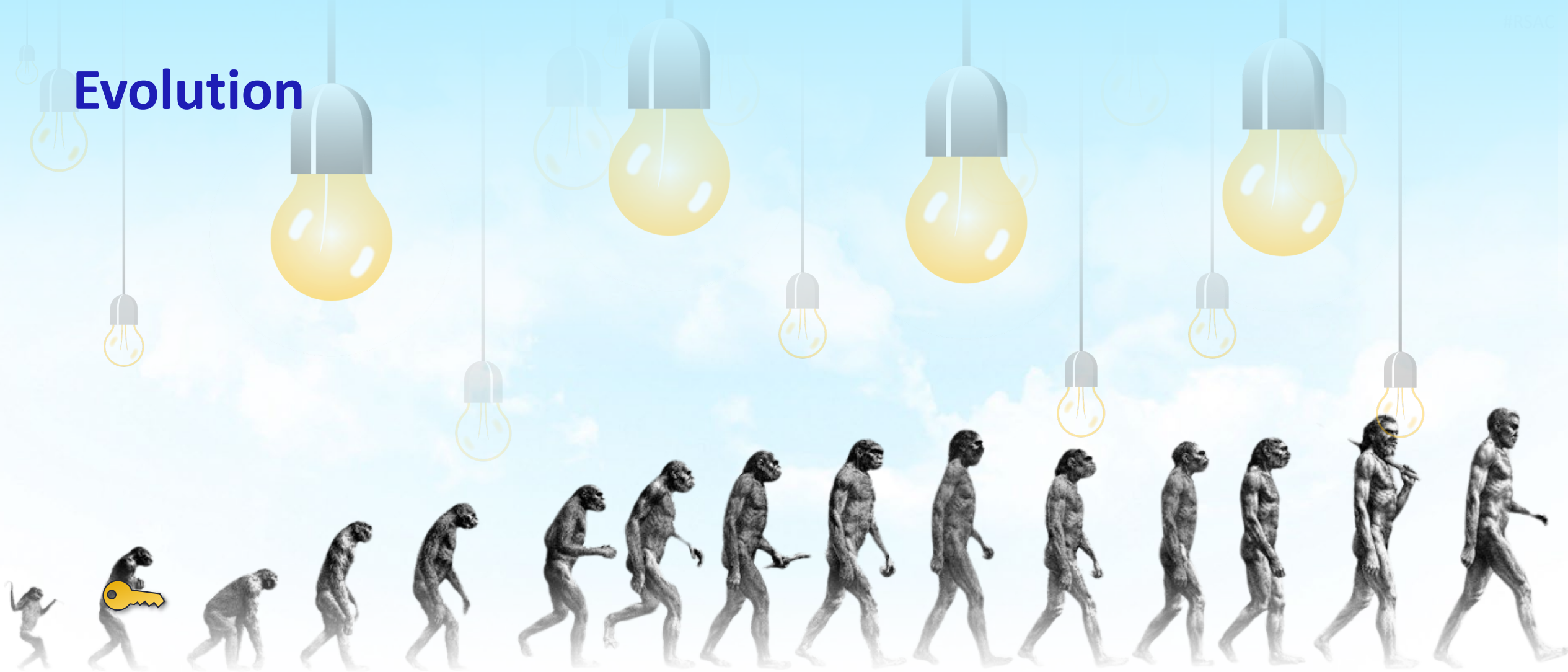
Evolution



2016 2023

From *Early Man* (1965; revised 1968), by F. Clark Howell. Illustration, "March of Progress," by Rudolph Zallinger.

Evolution



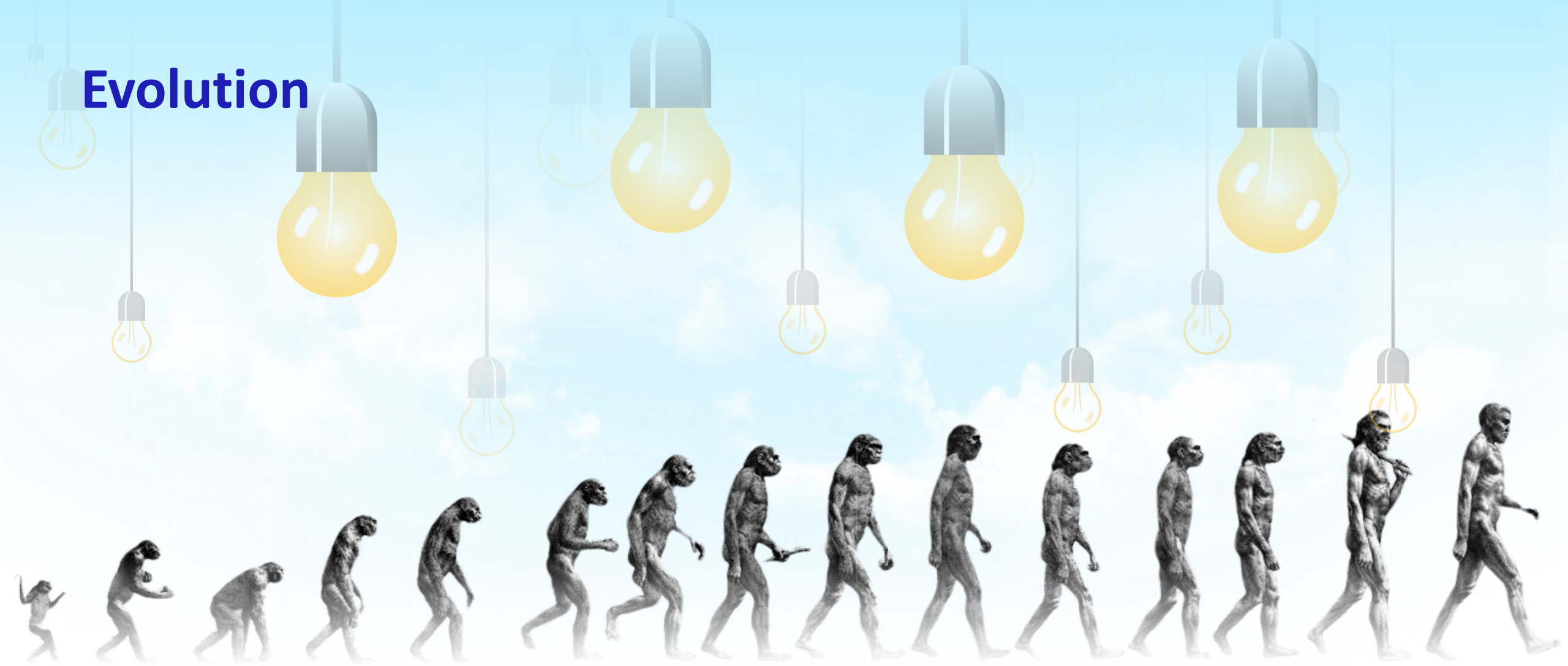
2016 2023

Microsoft

RSAConference2024

From *Early Man* (1965; revised 1968), by F. Clark Howell. Illustration, "March of Progress," by Rudolph Zallinger.

Evolution



2016 2021 2023

STORM 0558

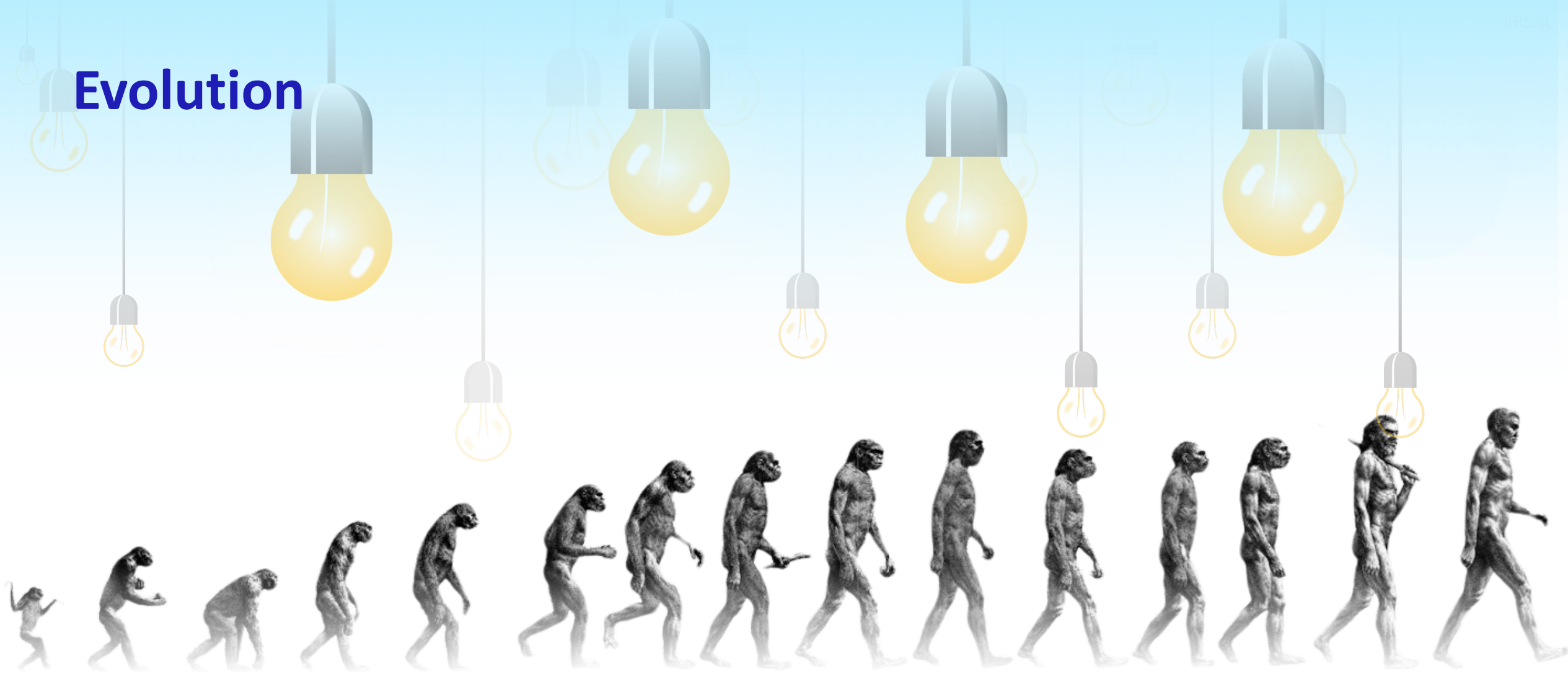
?

Microsoft

RSAConference2024

From *Early Man* (1965; revised 1968), by F. Clark Howell. Illustration, "March of Progress," by Rudolph Zallinger.

Evolution



2016 2021 2023

Log expiration / Sweeper processes

STORM 0558

?

From *Early Man* (1965; revised 1968), by F. Clark Howell. Illustration, "March of Progress," by Rudolph Zallinger.

September 6, 2023

Primary lines of investigation exhausted

Microsoft | MSRC Report an issue Customer guidance Engage

Results of Major Technical Investigations for Storm-0558 Key Acquisition

MSRC / By MSRC / September 06, 2023 / 5 min read

March 12, 2024 update

As part of our continued commitment to transparency and trust outlined in Microsoft's Secure Future Initiative, we are providing further information as it relates to our ongoing investigation. This new information does not change the customer guidance we previously shared, nor have our ongoing investigations revealed additional impact to Microsoft or our customers. No additional customer action is required.

On July 11, 2023, Microsoft published the results of our preliminary investigation into activity by the threat actor group Storm-0558, a threat actor operating from China. On September 6, 2023, we announced that major technical investigations were complete.

However, we continued to research the threat actor's tactics and techniques to help ensure customers were protected from similar attacks. Today we are providing this addendum to clarify and ensure the accuracy of our content based on our latest knowledge.

First, what hasn't changed:

The response

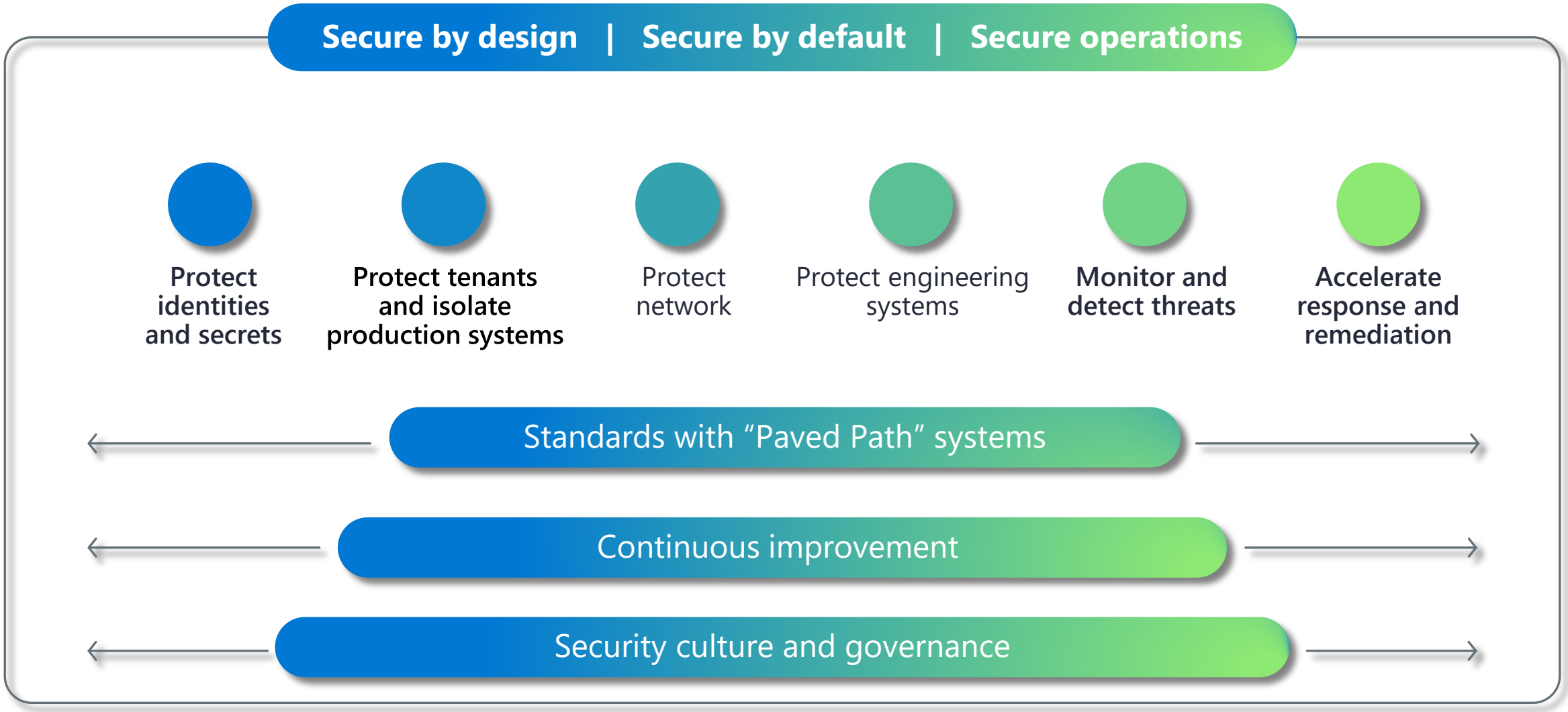
If you're faced with the tradeoff between security and another priority, your answer is clear: **Do security**.

—Satya Nadella

Microsoft

RSAConference2024

Secure Future Initiative



Secure Future Initiative

Secure by design | Secure by default | Secure operations

Protect identities and secrets

- Protect identity infrastructure signing and platform keys with rapid and automatic rotation with hardware storage and protection (for example, hardware security module (HSM) and confidential compute).
- Strengthen identity standards and drive their adoption through use of standard SDKs across 100% of applications.
- Ensure 100% of user accounts are protected with securely managed, phishing-resistant multifactor authentication.
- Ensure 100% of applications are protected with system-managed credentials (for example, Managed Identity and Managed Certificates).
- Ensure 100% of identity tokens are protected with stateful and durable validation.
- Adopt more fine-grained partitioning of identity signing keys and platform keys.
- Ensure identity and public key infrastructure (PKI) systems are ready for a post-quantum cryptography world.

The moral

Growth Mindset

The recent findings by the Department of Homeland Security's Cyber Safety Review Board (CSRB) regarding the Storm-0558 cyberattack from last July, and the Midnight Blizzard attack we reported in January, underscore the severity of the threats facing our company and our customers.

Microsoft plays a central role in the world's digital ecosystem, and this comes with a critical responsibility to earn and maintain trust. **We must and will do more.**

We are **making security our top priority at Microsoft, above all else**—over all other features. We're expanding the scope of SFI, integrating the recent recommendations from the CSRB as well as our learnings from Midnight Blizzard to ensure that our cybersecurity approach remains robust and adaptive to the evolving threat landscape.

aka.ms/SFIblog