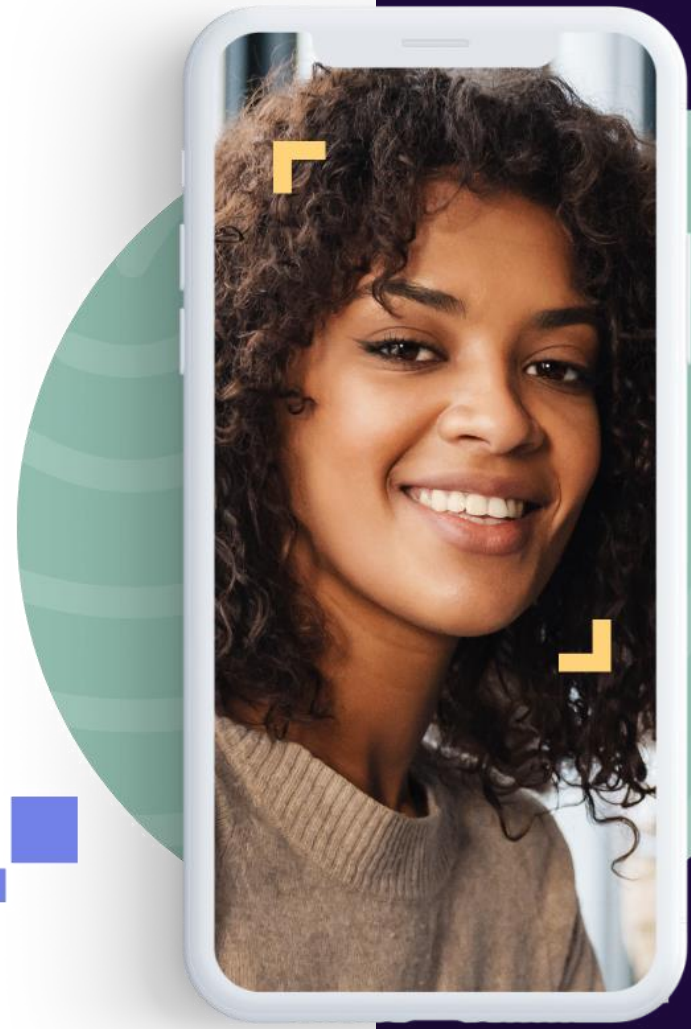
Zero Trust Digital Identity and Passwordless Authentication for Personnel and Individuals

Powered by Advanced Biometrics and Blockchain Technology



August 18, 2022

1KOSMOS

Sign Up Now.. Seats are Limited!

WEBINAR

MFA tried to fix Passwords but how do we fix MFA?

September 22, 2022 | 10:00 am PDT

1KOSMOS

Try the 1Kosmos BlockID Experience

www.1kosmos.com/demo

Install

- Download & install the 1Kosmos BlockID app for your device

Scan

- Use the 1Kosmos BlockID app to scan the QR code on this page

Enroll

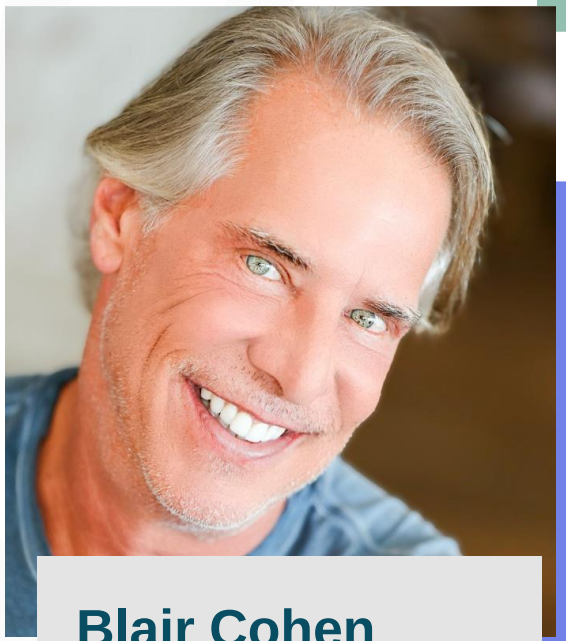
- Setup your biometrics profile on the 1Kosmos BlockID app

Authenticate

- Use biometrics to authenticate on the demo site

Today's Presenters

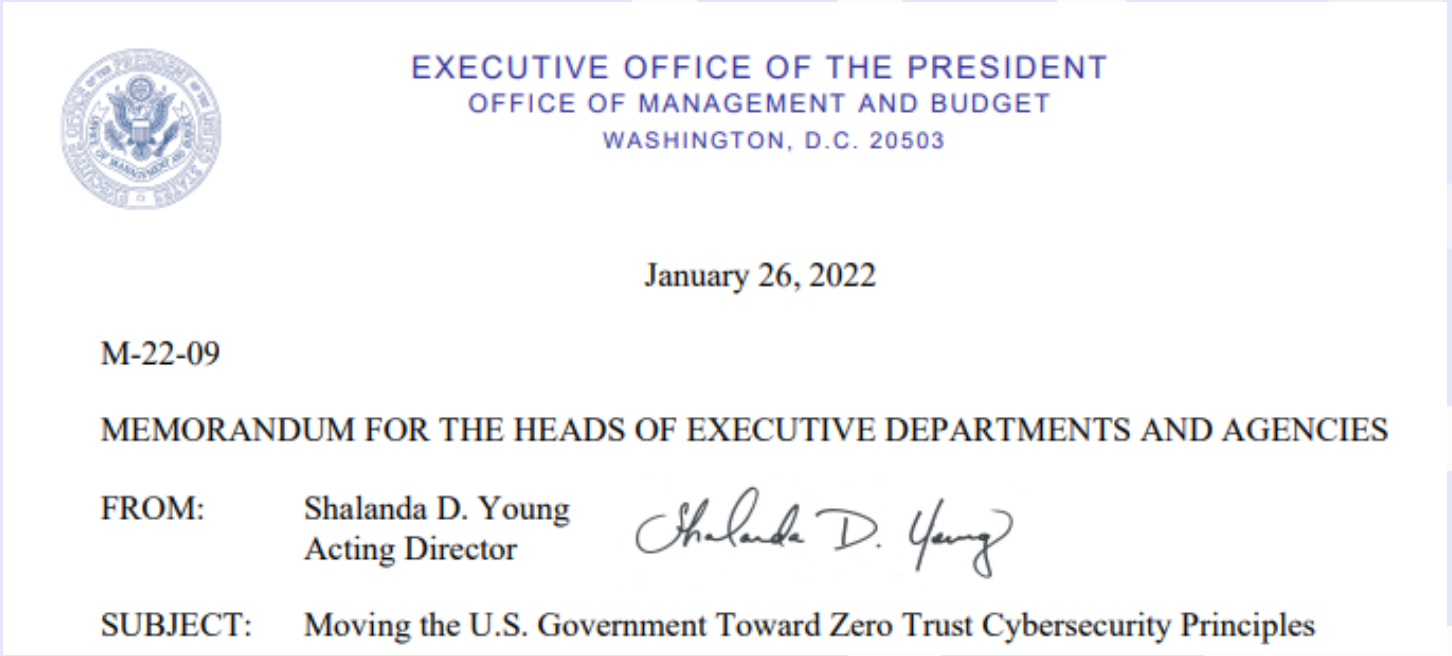
Mike Engle
Co-Founder, CSO
1KOSMOS



Blair Cohen
Founder & President
AuthenticID

Let’s talk Zero Trust

> “ Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

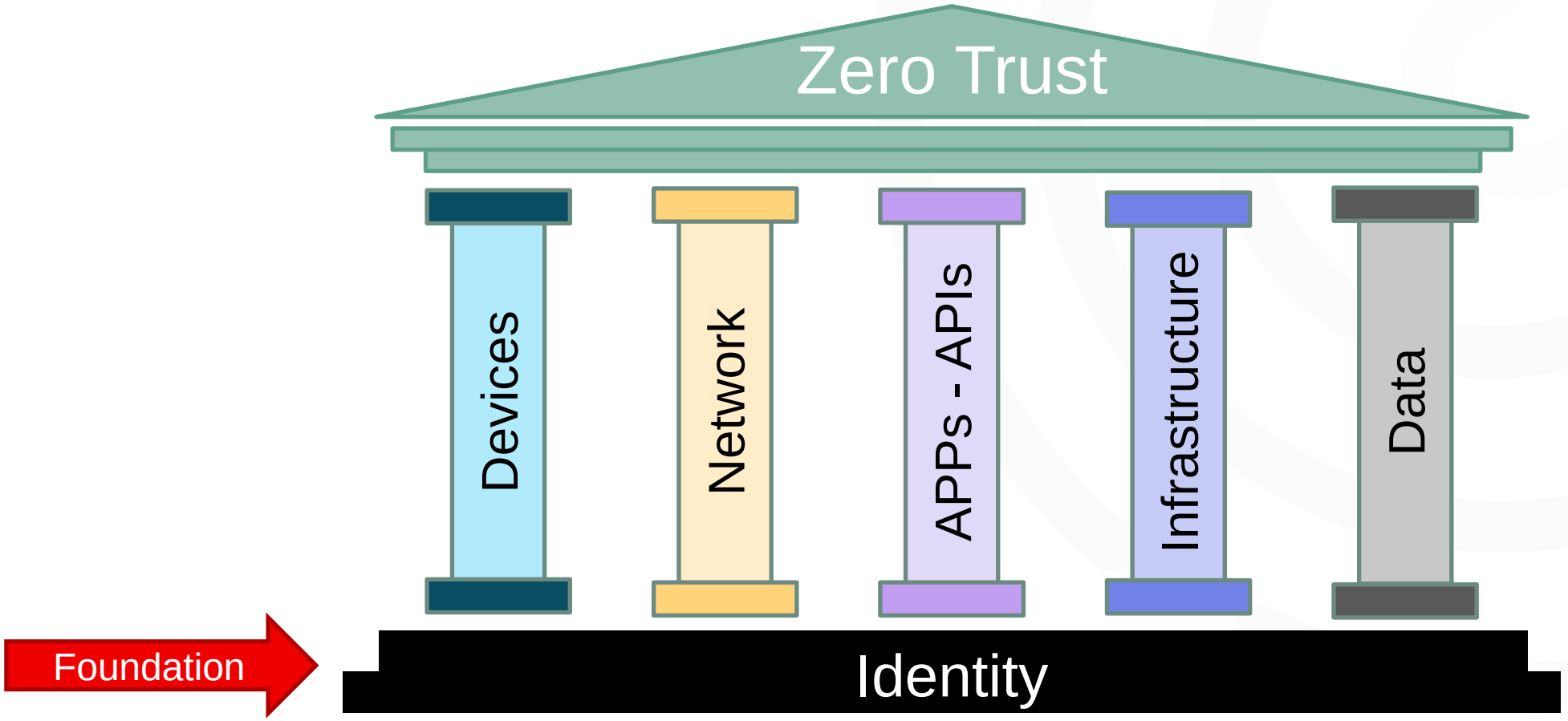
M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Components of a Zero Trust Framework



Passwordless MFA with Verified Identity

NIST 800-63-3A IAL

Prove who your employees and customers are

ESTABLISHES IDENTITY

How do you remotely PROOF someone?

- 2 forms of identity documentation
- Matched to REAL Biometrics

NIST 800-63-3B (AAL) + FIDO2 Passwordless

Grant them (and only them) to your systems

ENFORCES AUTHENTICATION

How do you remotely AUTHENTICATE someone?

- A private key, given to the user
- Matched to REAL Biometrics

kantara INITIATIVE Certified

iBeta QUALITY ASSURANCE Biometric Certified

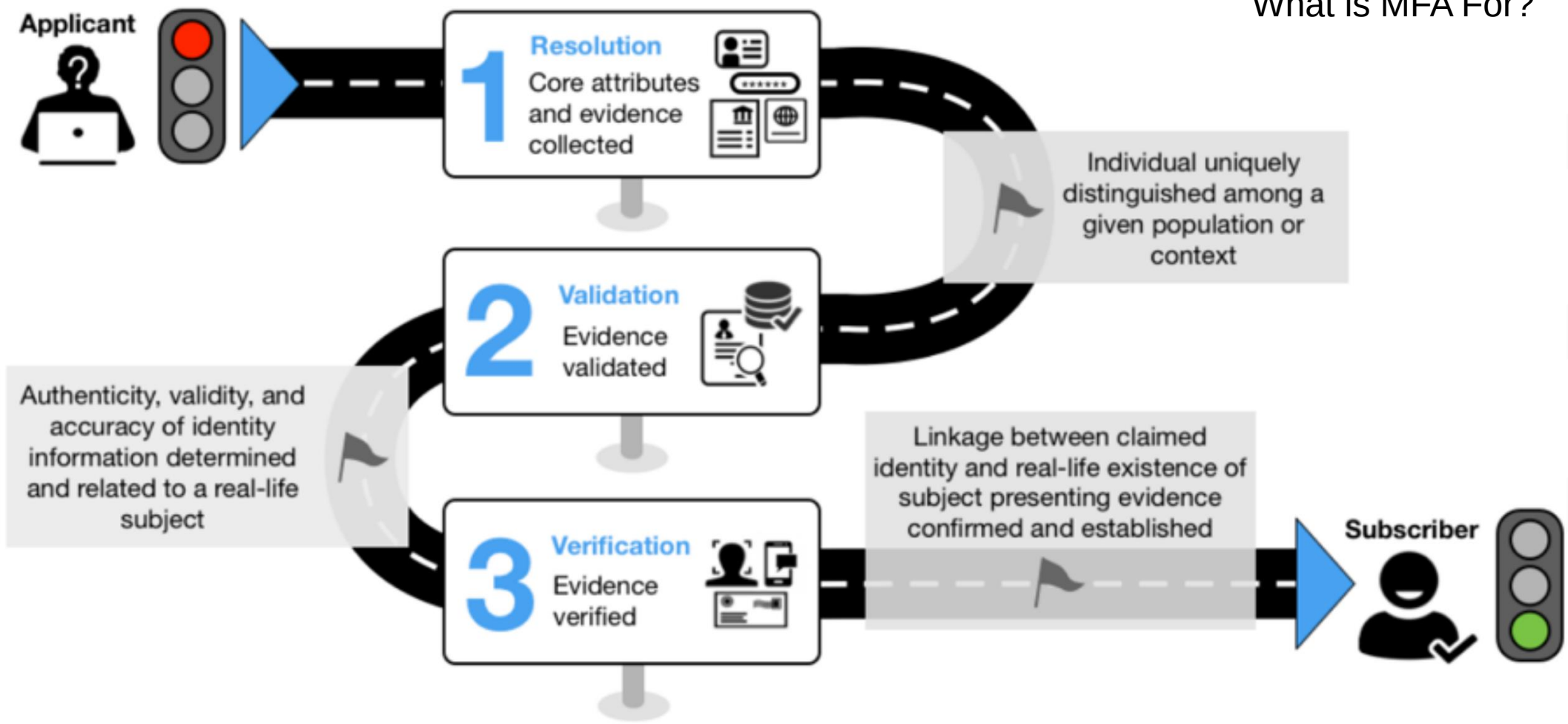
Identity-Based Authentication

fido CERTIFIED

NIST 800-63-3 Identity Standard

“ Agencies must use strong MFA throughout the enterprise.

What is MFA For?



Identity Assurance Level

What is IAL?

Identity Assurance Levels (IALs) are a key component of the(NIST) Digital Identity Guidelines, NIST 800-63-3. The standards are used by federal agencies to verify that people are who they say they are before being granted access to restricted information or accounts.

Automated ways to get to IAL2

NFC Passport + LiveID
Driver's License + AAMVA verification
Driver's License + SSN Verification

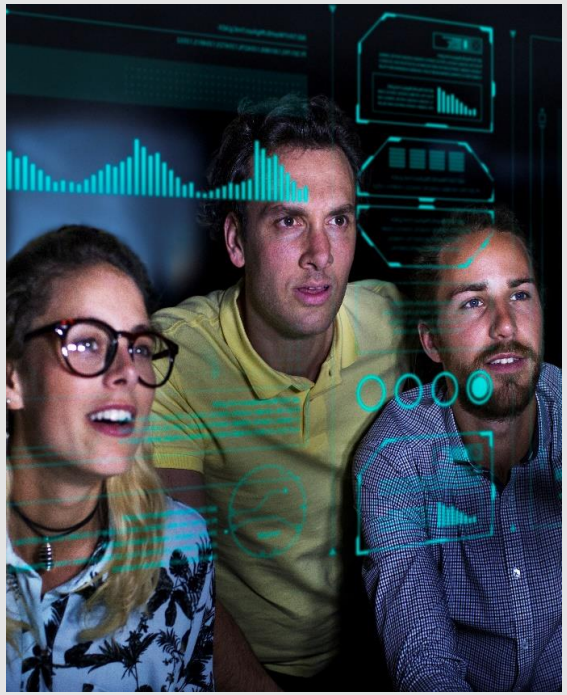
Identity Assurance Levels

IAL 1	• No identity evidence is collected.
IAL 2	• **One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with the issuing source, or** • **Two pieces of STRONG evidence** • **One piece of STRONG evidence plus two (2) pieces of FAIR evidence**
IAL 3	• Two pieces of SUPERIOR evidence, or • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with the issuing source • Remote (FIPS 201-3) or in-Person Certification – BlockID Attestation is available.

IAM's Missing Function: Proof

> Agencies must enforce MFA at the network and application layers.

USERS



Upon **Access**

Cryptographic Proof of Identity

Upon **Audit**

Cryptographic Proof of Identity

Zero Trust **MUST** Answer "Who" with authority

IT Functions

ID Governance/ Access

SailPoint · SAVIYNT · workday. · PeopleSoft

Single Sign-On

okta · PingIdentity · Microsoft Azure · ForgeRock

Privileged Access

CYBERARK · thycotic · Centrify ZERO TRUST PRIVILEGE · Hitachi ID

OS, Remote Access

zscaler · citrix VPN

How do you enforce identity at the endpoint?

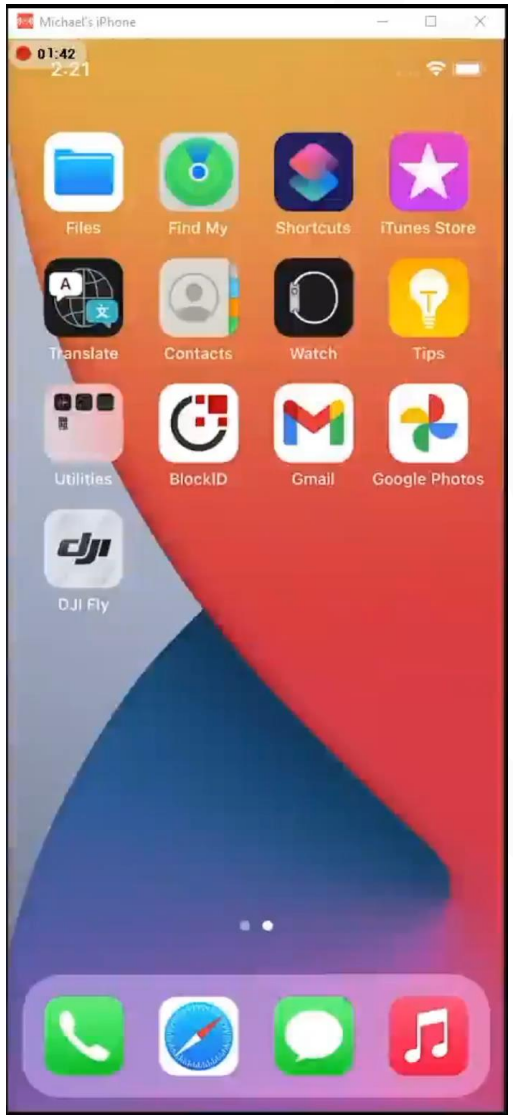
> Agencies must ensure their endpoint detection and response (EDR) tools meet CISA technical requirements and are widely deployed.

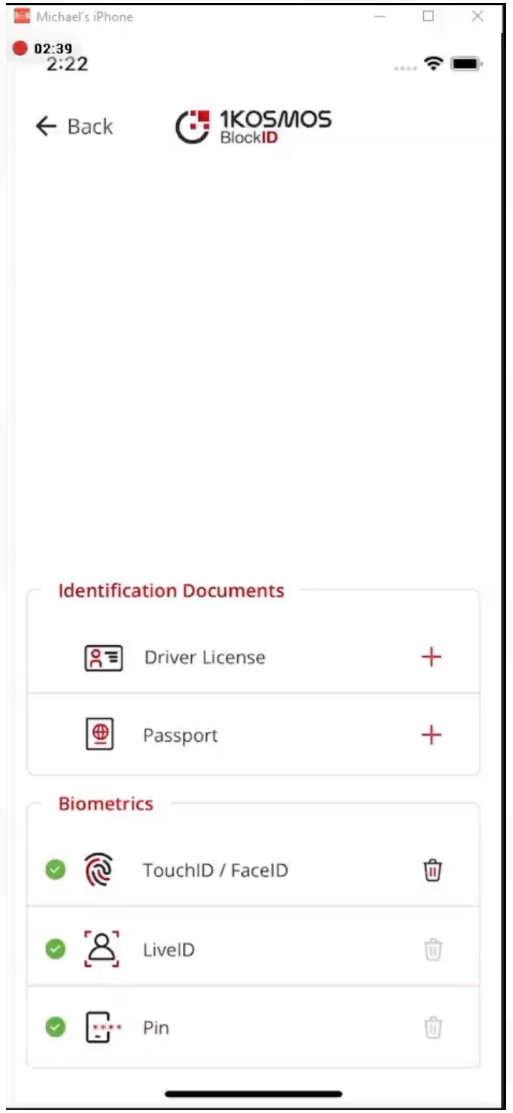
Demo – Identity & Biometric Enrollment

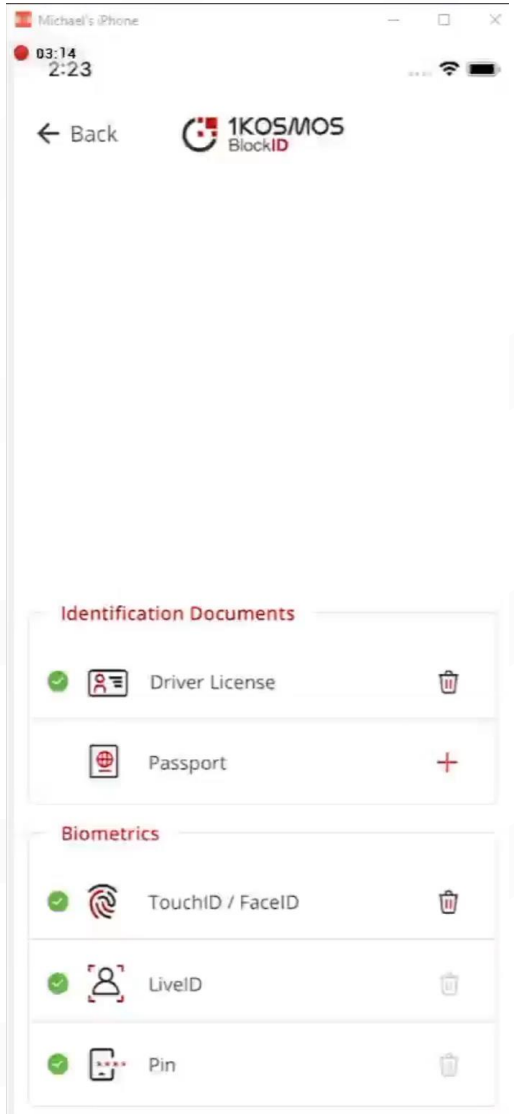
1) Launch App
   a. Private key generated and stored in TPM
   b. PIN created
   c. TouchID/FaceID Device Biometrics
   d. LiveID Real Biometrics

2) Verify 1st credential (driver's license)
   a. Real-time processing
   b. Face matched with LiveID
   c. Document verified with 3rd party sources
   d. Overt security features validated

3) Verify 2nd credential (passport)
   a. RFID chip is scanned
   b. Face matched with license & LiveID
   c. Passport digital signature verified
   d. Overt security features validated







Can the government agencies use this?

The New GSA "Identity Lifecycle Management Playbook" calls out FIDO and WebAuthn

This Continues the trend of US government agencies embracing FIDO in guidance and policy – the US General Services Administration (GSA) published a new Identity Lifecycle Management Playbook targeted at helping Federal agencies better manage enterprise identity systems that specifically details the critical role FIDO plays in these systems.

A blog discussing the Playbook is at
https://www.gsa.gov/blog/2022/08/12/modernize-your-identity-management-process-through-ilm

The actual playbook:
https://playbooks.idmanagement.gov/playbooks/ilm/

ID Creation: New User - GovID + 3rd Party Verification

Enrollment/Onboarding

ID Data Extraction

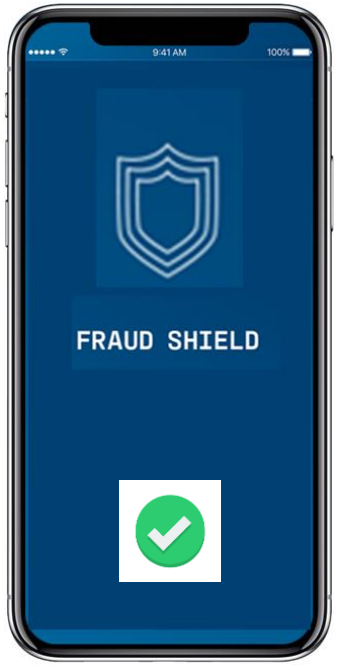
Instant data extraction from front and back of ID

ID Authentication

Verification of ID security features and detection of fraudulently tampered ID's

Selfie Facial Match/Liveness

Selfie Match to ID Photo plus liveness validation



Fraud Screening

Screening against known fraudster and criminal databases

Identity Verification

Multiple Data Sources

Compare user-asserted or document data from multiple 3rd parties with one API call.

Non-Bias Facial Recognition

Document Authentication *without* ID to selfie match

	False Accept Rate (FAR)	False Reject Rate (FRR)
Caucasian	3.02%	2.94%
Non-Caucasian	2.93%	2.20%
Male	3.09%	2.66%
Female	2.65%	2.73%

There is no biometrics in this sample set: Rejection rates are attributed to document performance and capture performance in terms of dirt, damage, wear and capture quality.

Document Authentication *with* ID to selfie match

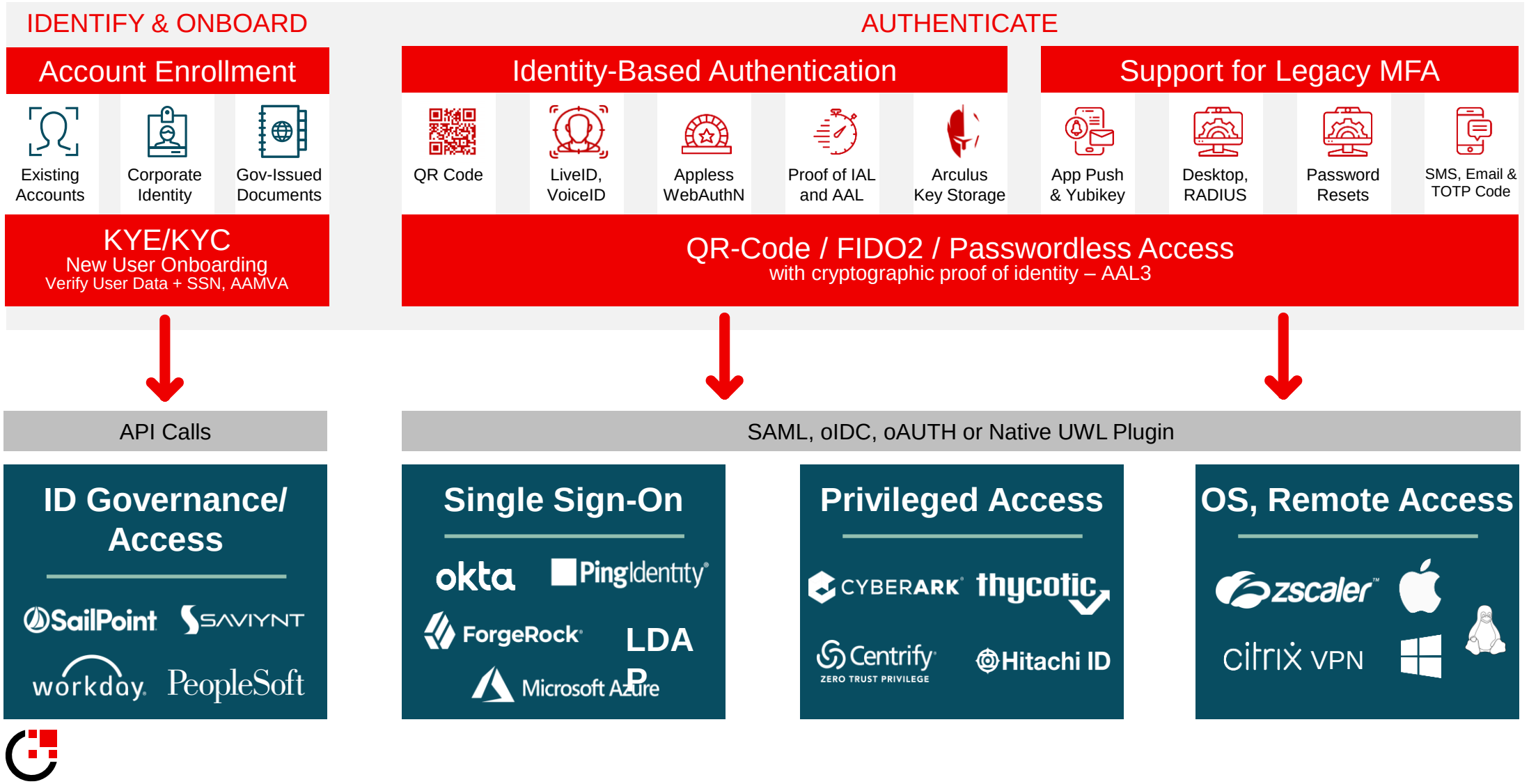
	False Accept Rate (FAR)	False Reject Rate (FRR)
Caucasian	0.2%	2.7%
Asian	0.2%	2.49%
African	0.41%	2.91%
Male	0.2%	5.29%
Female	0.62%	2.91%

Error rates of facial recognition matching of a selfie to ID headshot related to FAR where a fraudulent/tampered document or presentation attack is presented and passed as Verified. FRR is when a genuine ID presented with a selfie is falsely rejected as a facial non-match, counterfeit, false presentation attack, or tamper attempt.

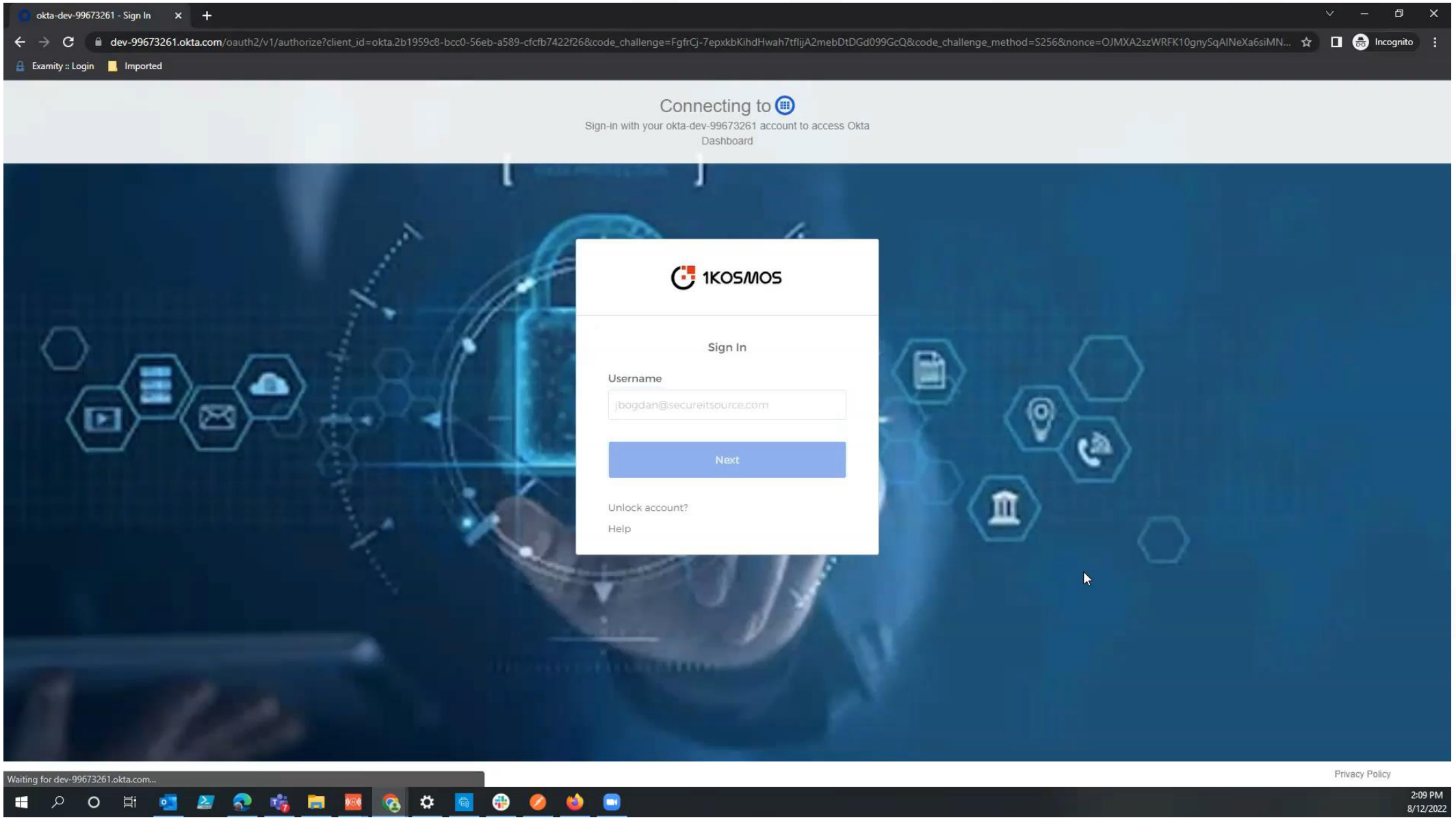
Your MFA must be flexible and have ADMIN-X!

> Agencies must develop a zero-trust architecture (ZTA) plan that describes the agency's approach to environmental isolation (in consultation with CISA) and submit it to OMB as part of its ZT implementation plan.

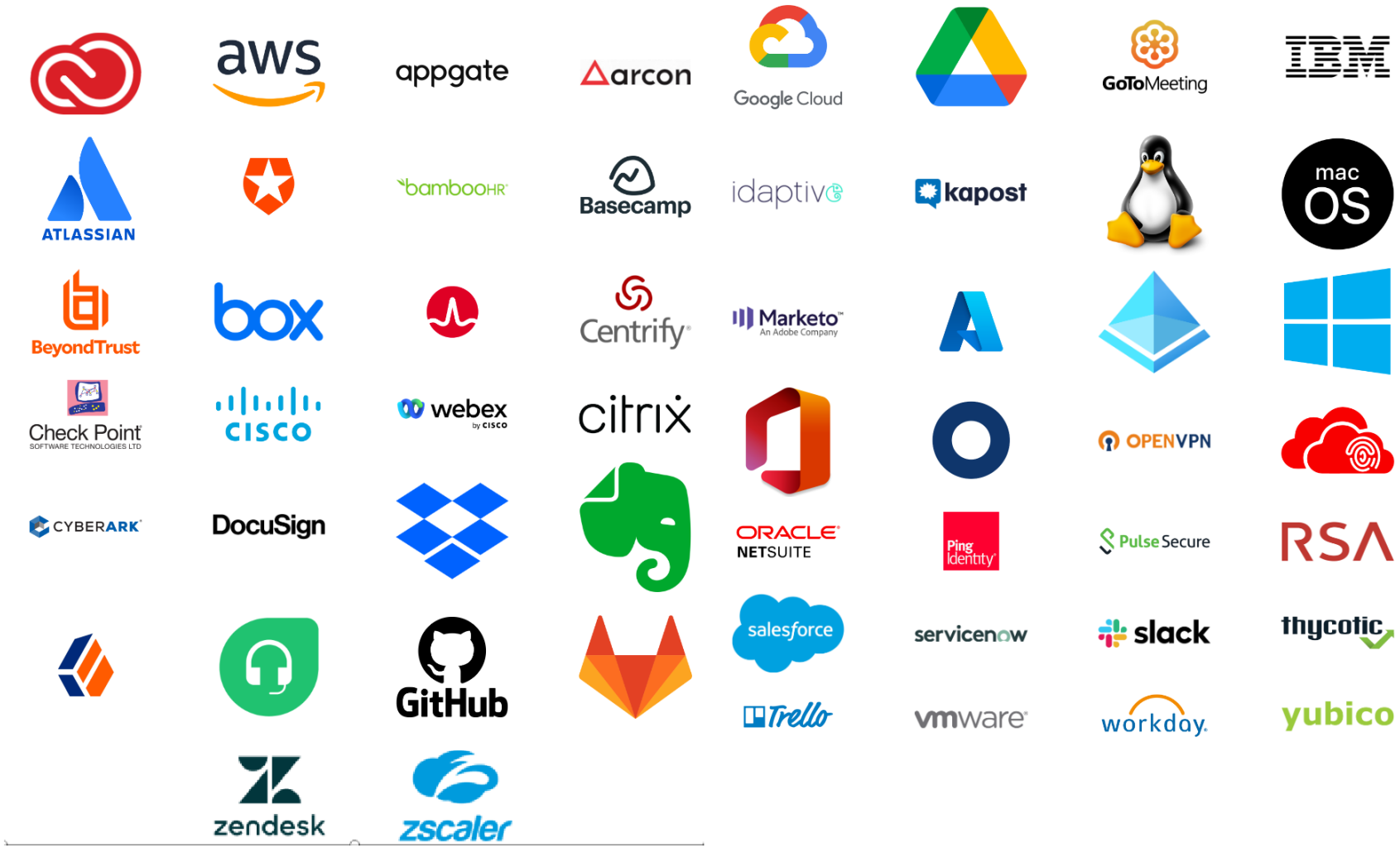
Identity-Based IAM Reference Diagram



Demo – Zero Trust Authentication into SSO



Out-of-the-box Connectors



Deployment Considerations

> What training is needed to implement the proposal by addressing both the technical staff and the users?

Self-evident user onboarding & administrative experiences reduce training requirements.

K.I.S.S. 3-Step Approach to Adoption

> A Zero Trust Authentication system should be deployed in Parallel, not as a cutover.

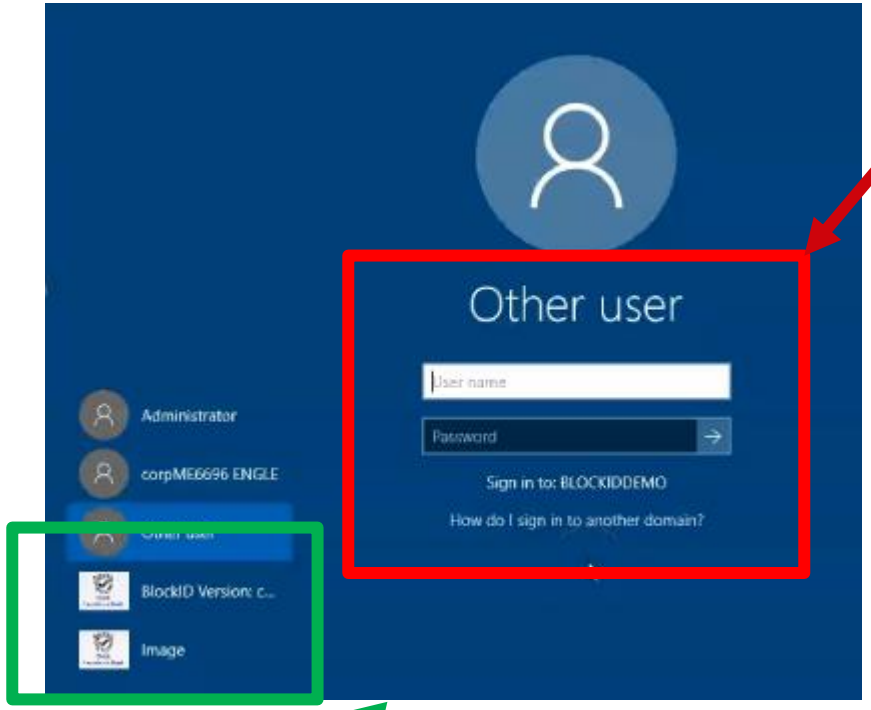
Sounds Great! Now What?

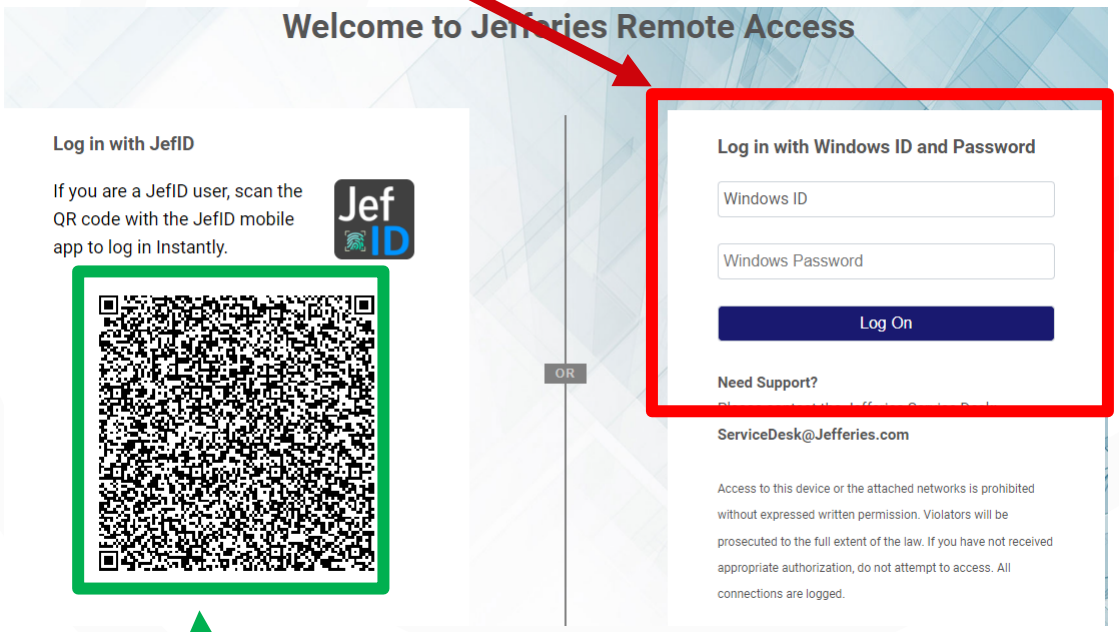
3 Systems = 80% of the MFA surface

1. Remote Access
2. Operating Systems
3. SSO Gateways

Side-by-side deployment

Support Legacy 2FA Auth





ZTA Identity Auth

How It Works: For IT

1

BlockID platform is set up

- Enable web resources (on-prem IDP, Cloud/SSO system, Citrix immediately
- Existing IT system change: None

Install in 5 minutes

2

80/20 target systems are connected
(typically Windows/Mac, Remote Access, and a SSO Gateway)

- AD broker uses the existing proxy infrastructure for outbound connections only

Production in 1 week

3

Users are invited into the platform and “self enroll” at any pace

- Completion time: As soon as desired
- Existing IT system change: None

Onboard users with 1 click

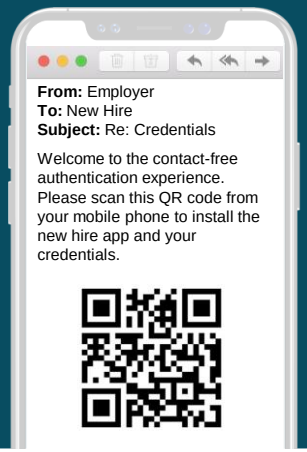
Day 2: Remove 2 legacy auth systems

- ✓ **No DMZ Components**
- ✓ **No Firewall Changes**
- ✓ **Fast Risk Review Process**

How It Works: For Users

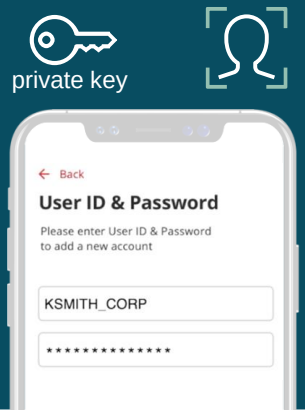
1

User is invited to the system via magic link on phone



2

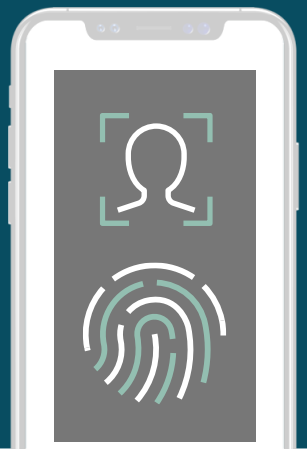
User enters existing company credential(s) **one last time and enables biometrics**



Self-enrollment in <1 minute

3

User authenticates **without** username/ password



Authentication in 1 second

Day 1: Target Systems

zscaler™

citrix

VPN

SSO

Deploys in parallel to existing authentication, no impact to production.

K.I.S.S. 3-Step Approach to Adoption

> Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB M-21-31 where the advanced level would be needed to support ZTA tenets.

Every Authentication should PROVE user identity.

FIDO or similar Private Key
Issued to User

Signature is written
to the server

E63318 B1AF8 318

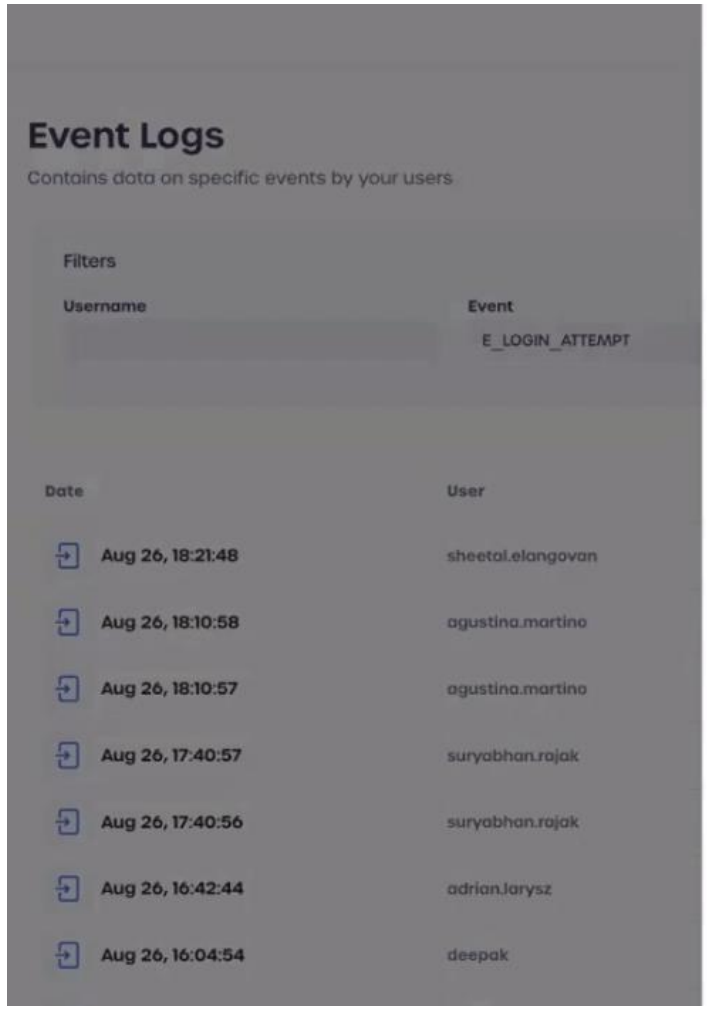
Biometric Verified, Encrypted
with User Private Key

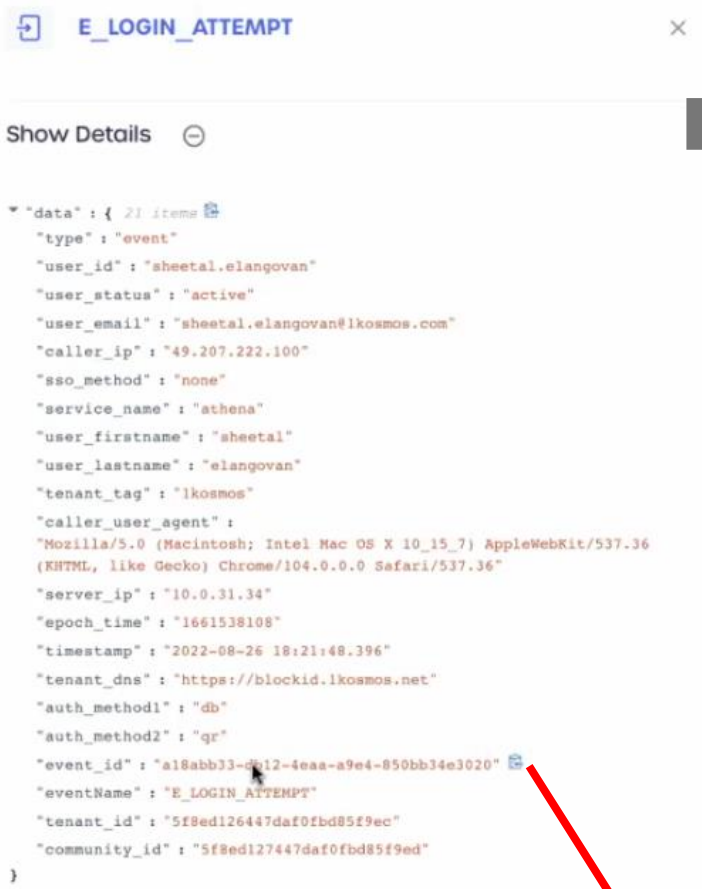
Signature is written
to the server

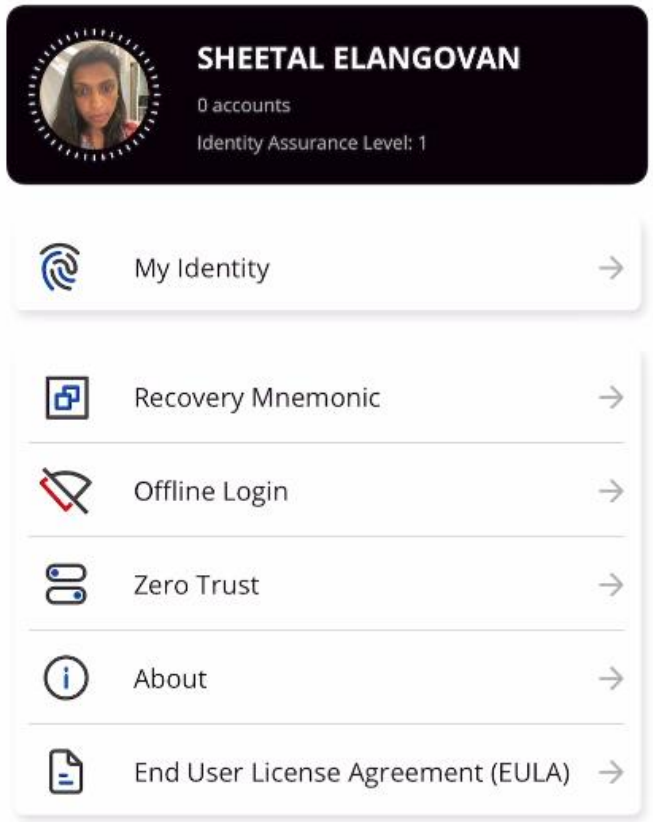
6FE2A 41CC24 1BA

These cryptographic signatures can be verified upon entry or post-access – every time.

Logging – cryptographically tied back to users



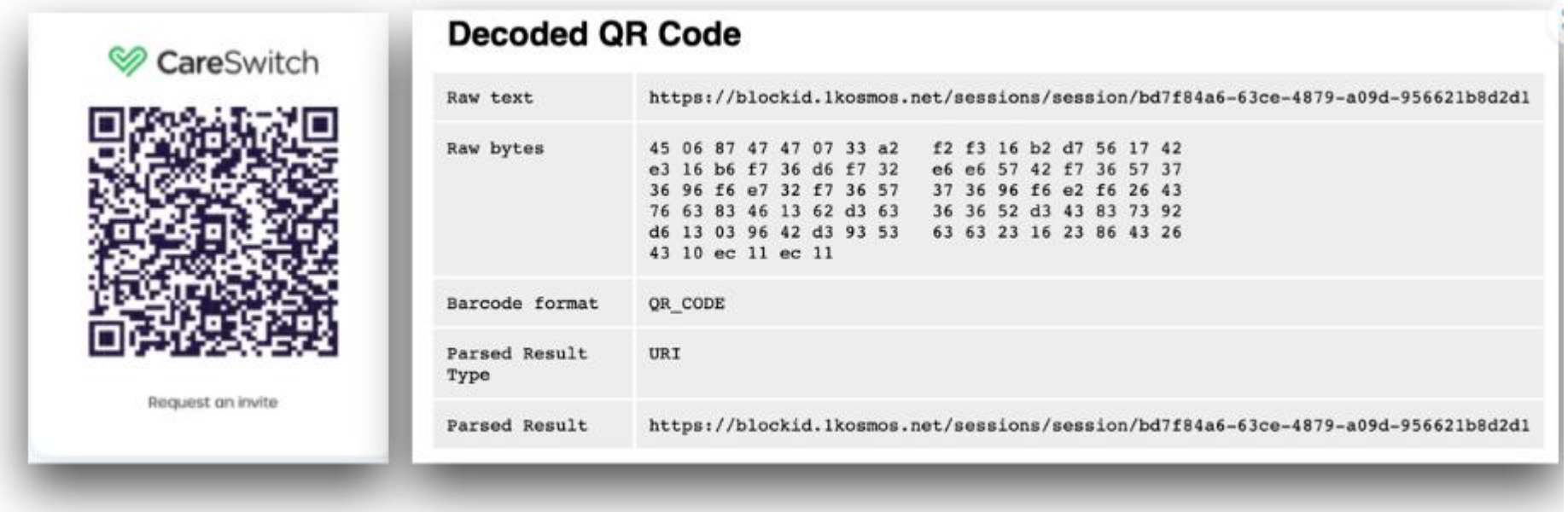




Blockchain logging ensures immutability.

Turnkey & Developer Solutions

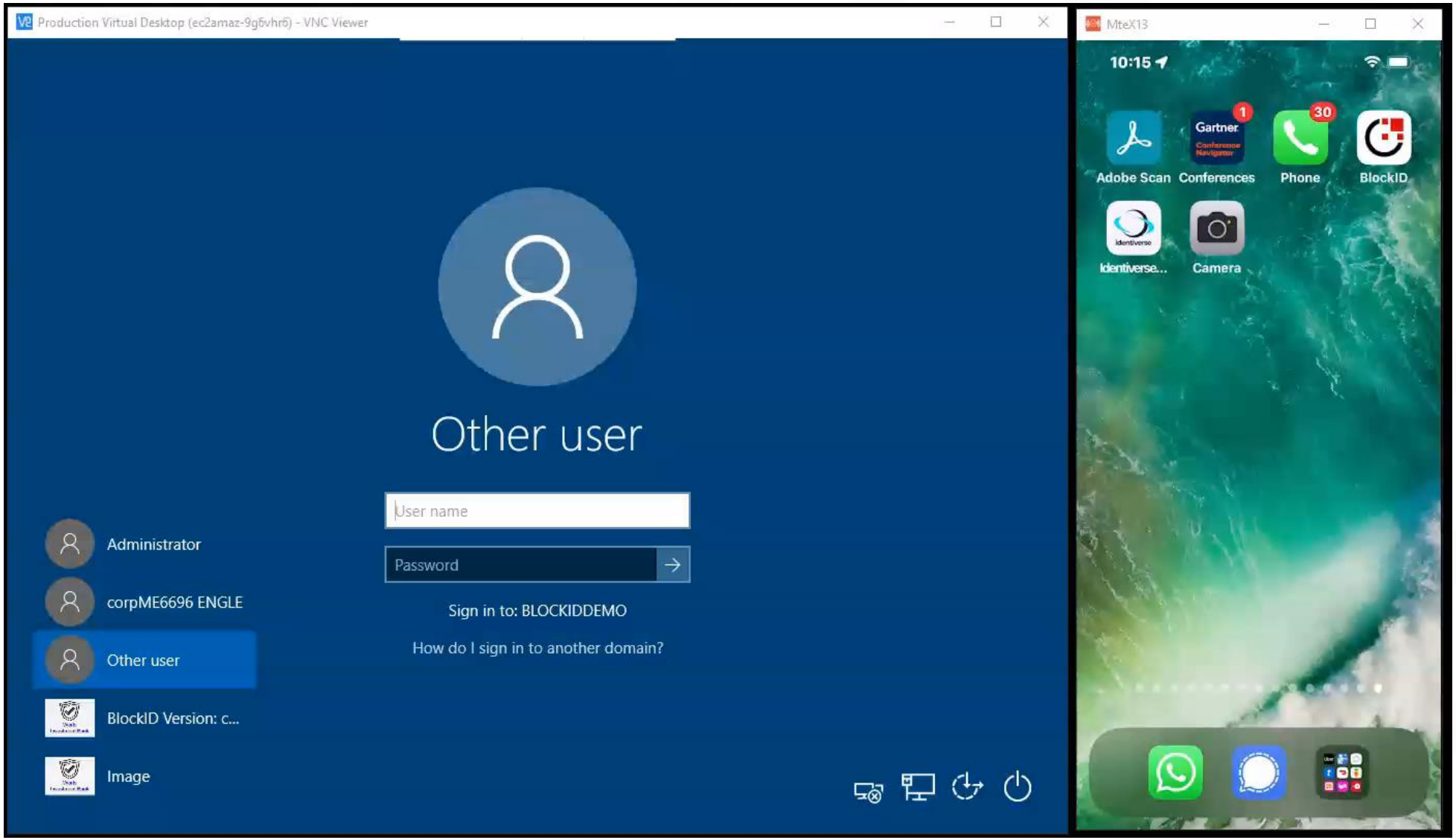
With a few lines of code, any web-based system can achieve Identity Based Authentication for ZTA



https://developer.1kosmos.com/

Demo – Identity-Based Authentication

Link to video



Total cost of operation

> What are your procurement and implementation costs?

Costs and ROI

- Services are deployed as a SaaS model.
- Given the guidelines of 60,000 total users and guidance of a $3m budget, 1Kosmos expects to be under budget for this project by over 30%.

Quantifiable ROI:

- Legacy MFA costs are reduced/removed
- Helpdesk costs are reduced (30% in first year, $50/call average, user productivity)

“Soft” ROI

- User experience (Customer satisfaction) improvements – 70% increase
- Reduction in authentication risk (ransomware, BEC, etc.)

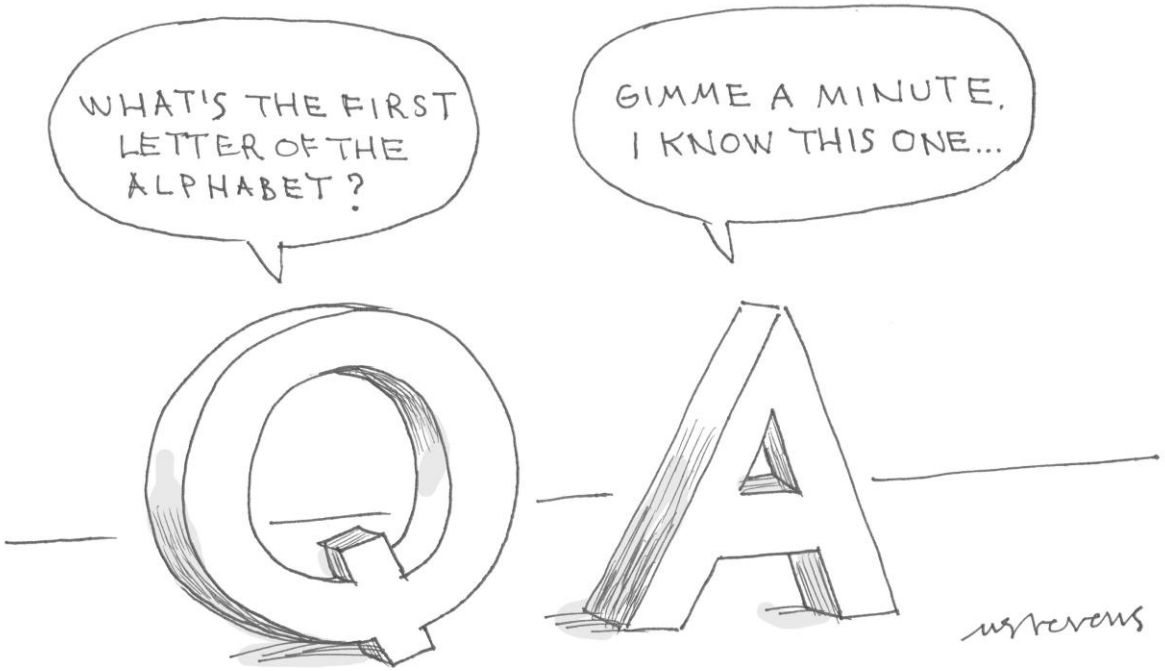
Identity Onboarding - Considerations

- **Data Privacy – who owns the Identity Data? Where is it stored?**
- **Is the data reusable (Proof once, use many)?**
- **Is the biometric certified for NIST 800-63-3, PAD, and Bias?**
- **Does the solution have global document coverage?**

Things to think about

Is SSO Enough?	SSO is only as strong as its authentication (Username? Password? 2FA?) … and protection of its master key (Solar Winds!)
Will users and companies trust real biometrics .. beyond TouchID/FaceID?	When done right (in the user's control, audited, and properly disclosed) – there is nothing to be afraid of.
How do I get started with Zero Trust?	In a phased, bite-sized approach – ordered by risk prioritization.

Q&A


WHAT'S THE FIRST LETTER OF THE ALPHABET?
GIMME A MINUTE, I KNOW THIS ONE...
Q
A

Thank You

Michael & Blair

Carnegie Mellon University
Software Engineering Institute

SEI Zero Trust Industry Day

Request for Information (RFI)

Prepared by:

Michael Engle
CoFounder & Chief Strategy Officer
1Kosmos, Inc.
michael@1kosmos.com
+1 7328200096

The purpose of this RFI is to gather proposals for providing guidance to U.S. federal agencies that must transition to a zero trust (ZT) cybersecurity strategy to address the Office of Management and Budget Memorandum (OMB) OMB M-22-09 (Moving the US Government Toward Zero Trust Cybersecurity Principles), which calls out OMB M-21-31 (Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents) based on this scenario:

> *A large U.S. federal agency provides services used by global users. The agency currently is operating a hybrid, multi-cloud enterprise that supports about 45,000 federal employees and 15,000 contractors. The enterprise's networks break down into Information Technology (IT) (75%), Operational Technology (OT) (15%), and Supervisory Control and Data Acquisition (SCADA) (10%). The OT and SCADA networks support the agency's smart buildings' controls/operations and distribution centers.*
>
> *Currently, the agency has identified three high-value assets (HVAs): two legacy systems and one database containing Protected Personal Information (PPI). The agency is currently using four different identity and access management systems (Okta Identity Cloud, Cirrus Identity, Azure AD, and Google Cloud Identity) and lacks a centralized security operations center (SOC).*
>
> *The agency is currently unable to integrate logging information due to the continued use of legacy systems: an organizational structure where SOC operations are broken across different teams and a hybrid, multi-cloud implementation where services provide different formats for the information. The agency must implement two-factor authentication but also must provide multi-factor authentication (MFA) for some parts of the enterprise.*
>
> *The agency has a budget of $3 million and a one-year timeline during which it must start to address M-22-09. Given this last constraint, each proposal should address its compatibility with the agency's existing hardware and software infrastructure.*

You must address the following specific OMB M-22-09 requirements in your proposal:

1. Identity
   a. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.

Our platform, BlockID, is a user-centric and "privacy by design" system that allows agencies to definitively prove who a user is before they are allowed access to common platforms.

Today agency systems have their own database but no way to prove a user's identity. However, the government and security industry have released several standards allowing agencies to solve this problem. These standards include:

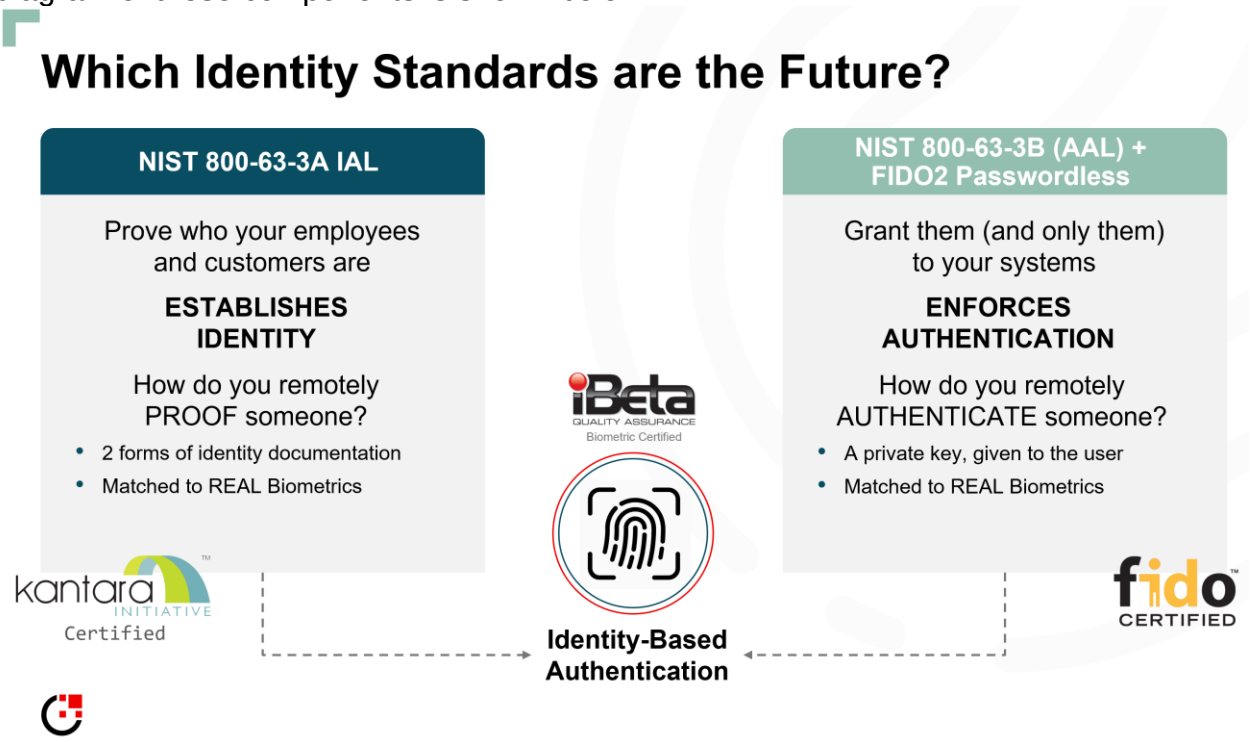
- NIST 800-63-3 - Digital Identity Guidelines
- FIDO2 Passwordless Authentication by the FIDO alliance
- SAML2, oAUTH2, OpenID Connect - to enable the sharing of identity attributes across systems

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

When done properly, an "identity layer" can be introduced without redesigning the target systems simply by configuring them to use these industry-standard protocols. This approach has several advantages:

- Avoids vendor lock-in - a standards-based approach ensures you can add/change vendors over time
- Lower system administration costs - By leveraging these standards, existing systems can be enhanced simply by configuring a new identity provider

This approach is referred to as "Identity-based authentication". It combines the use of public-key technology with user biometrics to prove who a user is before they are allowed to access a system. A diagram of these components is shown below:



b. Agencies must use strong MFA throughout the enterprise.

All systems, legacy and new, should employ the use of multi-factor authentication (MFA). The forms of authentication should include possession factors (security keys and other hardware factors), knowledge factors (passwords or secrets), and inherence factors such as biometrics. Examples of these factors include:

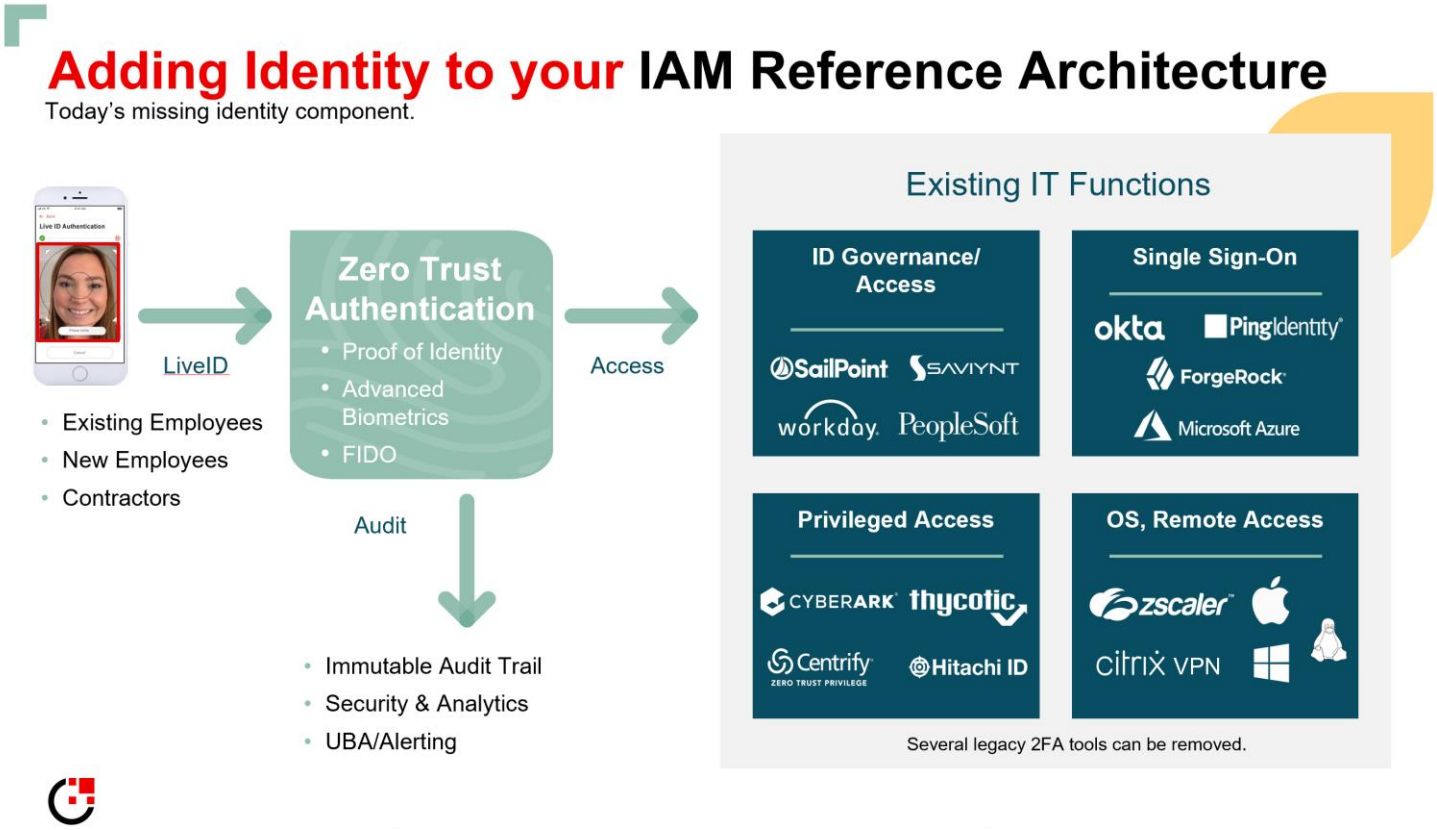
- One-time code generators such as TOTP - as long as these are generated with the user (on a device held by the user) and not sent via insecure channels such as email or SMS
- Device biometrics such as TouchID and FaceID
- Digital certificates including PKI (such as a smart card) or FIDO UAF authenticator

Note that the government has deprecated the use of one-time codes sent via text and email and these should not be considered as a strong form of MFA.

By selecting the right identity layer, agencies can use various MFA methods with the least amount of user friction possible. BlockID supports these and more MFA options with turnkey and developer-friendly approaches to make rapid deployment possible.

c. Agencies must enforce MFA at the network and application layers.

By leveraging industry-standard authentication protocols, the BlockID platform can be introduced both at the network layer and in applications. A common approach for adding MFA at the network layer includes adding to the organization's VPN stack and in front of workstations and servers. This diagram demonstrates how BlockID MFA can be added in front of any type of technology used in an organization:



2. Devices
   a. Agencies must create reliable asset inventories through participation in the Cybersecurity and Infrastructure Security Agency's (CISA's) Continuous Diagnostics and Mitigation (CDM) program.

Device inventory is out of scope for our product.

b. Agencies must ensure their endpoint detection and response (EDR) tools meet CISA technical requirements and are widely deployed.

An Identity-based authentication strategy compliments EDR by allowing for a strong "step-up" to prove user identity when an anomaly is detected. This approach can be applied to any end-user system.

3. Networks
   a. Agencies must develop a zero-trust architecture (ZTA) plan that describes the agency's approach to environmental isolation (in consultation with CISA) and submit it to OMB as part of its ZT implementation plan.

Entry points into the network should be configured to enforce identity levels of assurance before access is granted. For example, an agency could mandate that a user prove their identity (not just via username, password, and 2FA) with public-key cryptography and biometrics before they are allowed to VPN into a sensitive network.

To make the configuration of network access easy, RADIUS and SAML are supported as standard protocols. Integration with VPNs, Firewalls, Routers, Wireless controllers, web proxies, and DLP consoles are supported by BlockID where username and password are replaced with biometrics.

4. Data
   a. Agencies must implement initial automation of data categorization and security response, focusing on tagging and managing access to sensitive documents.

Data categorization is out of scope for our response.

   b. Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB M-21-31 where the advanced level would be needed to support ZTA tenets.

Secure logging of identity access is one of the most important aspects of a proper audit trail. The BlockID platform utilizes a distributed ledger to store access records, meaning that the audit trail is immutable. This mitigates the risk of bad actors changing log files to cover their tracks.

All logs can be accessed from our single unified administration console.

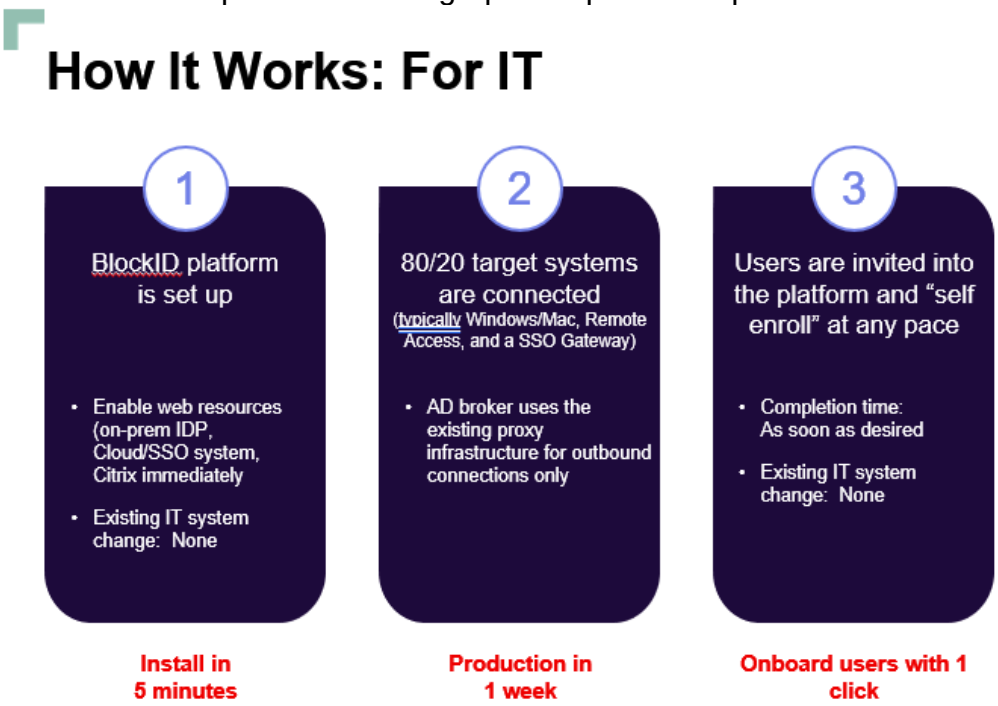
In addition to the above, logs are also maintained to the source of requests for data, the number of logins, the location of access, the device from which access is made, and the time and date of access.

We recommend that you produce and discuss the following artifacts and information in your presentation:

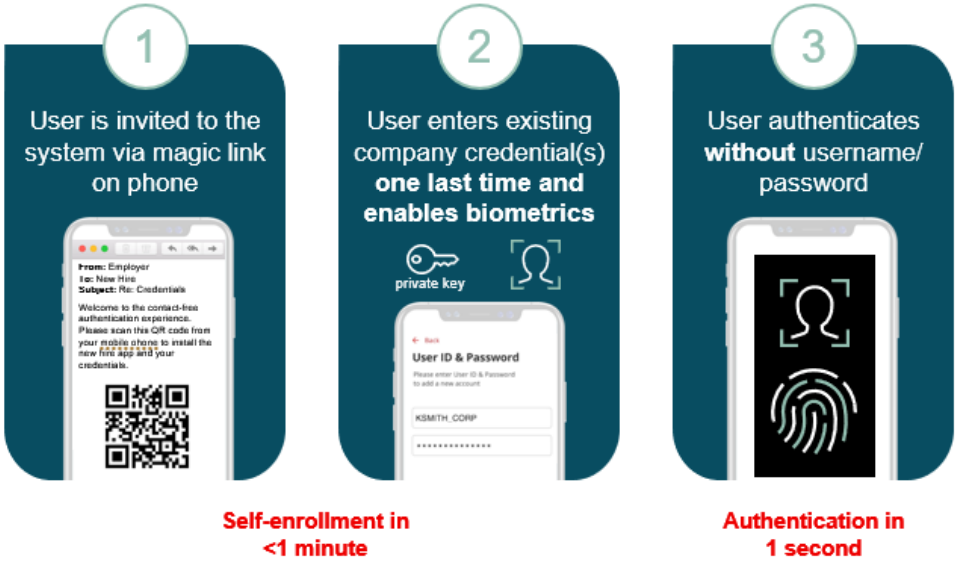
1. Cybersecurity architecture strategy to implement ZT
   a. How ZT tenets are prioritized based on requirements and impact to agency

By focusing on the Identity pillar of Zero Trust first, agencies can reap tremendous security benefits with the least impact to existing infrastructure and to users. A simple 3-step process allows for the adoption of identity-based authentication.

For IT administrators, existing systems can be connected in minutes via SAML, OIDC, and other standard-based protocols. This graphic explains the process:



For users, the process is very straightforward as shown here:



Typical candidates for day 1 are remote access and primary operating system computers. It only takes 30 minutes to connect to any cloud service. BlockID supports Windows, Mac, Unix, SAML, OIDC, oAuth so the time to get operational is minimal.

If an agency has on-prem resources to connect to such as Active Directory, we have a lightweight agent that goes on-prem. It does not need any DMZ components, firewall changes, or load balancers. It only makes outbound connections through your proxy and no corporate data or credentials are sent to the cloud. This lets the process move through your risk review very quickly.

Lastly, administrators will invite users into the system. This is done via the press of a button to send them the invitation and they will start the self-enrollment process.

b. Considerations

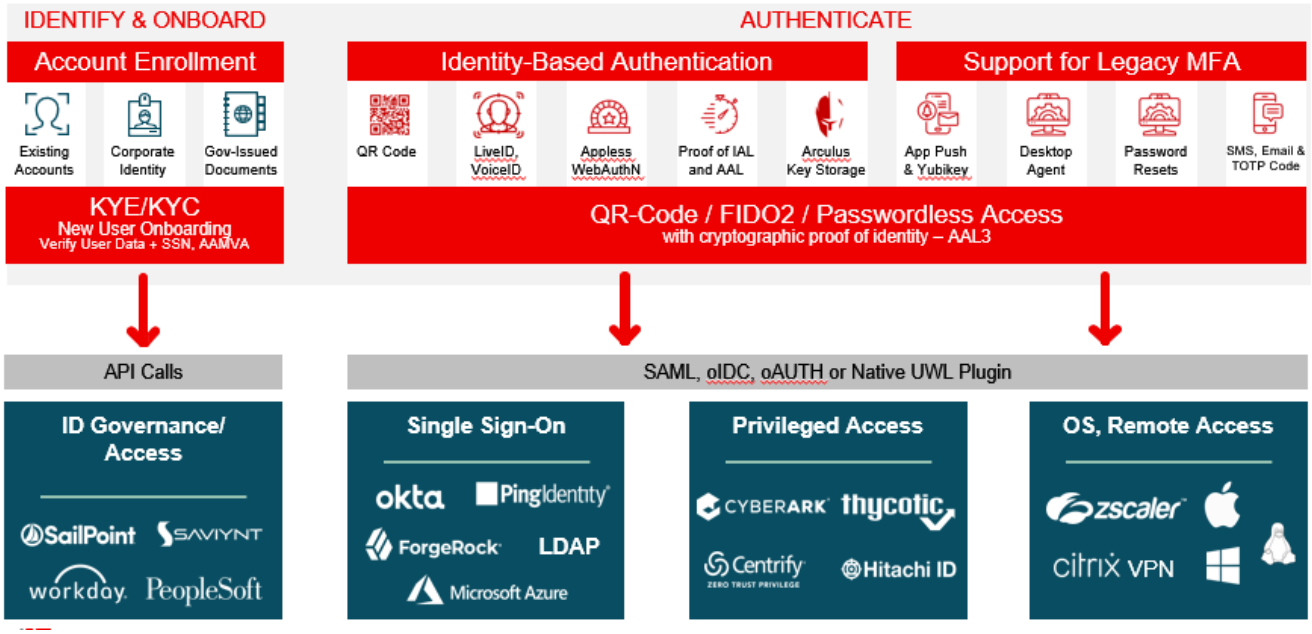
We have demonstrated that 80% of existing entry points for users can be covered in the first phase of deployment simply by focusing on the most used systems. For example, by covering remote access, operating systems, and SSO providers with identity-based solid authentication (public key + biometrics), a large percentage of attack vectors can be closed.

i. Support for a mixed environment or not for hardware (i.e., multiple vendor products)

By leveraging industry standards (NIST 800-63-3 and FIDO2), we allow for the interoperability of multiple vendor products including smart cards, Yubico devices, and other hardware-based tokens. This allows for the use of identity-based authentication even in SCIFs and other secure areas where mobile phones are not permitted. Vendor lock-in is also mitigated by adopting a standards-based approach for authentication protocols including SAML, OIDC and oAUTH.

ii. Software interoperability

The following diagram shows several integration options that allow for interoperability amongst various software products. The connectors in grey below the arrows indicate protocols used for integration. The functions in RED demonstrate new authentication capabilities that can be introduced to support zero trust for identity.



iii. Impact on data management

The introduction of a standards-based identity layer gives agencies one common authentication framework which simplifies the management of user accounts. Rather than relying on dozens of disparate user directors, there can now be one authoritative source for user access.

2. Two ZT roadmaps: one near-term (0-2 years) and one long term (3-5 years)
    a. Addresses OMB M-22-09 and M-21-31, the CISA Maturity Model, CISA Trusted Internet Connection (TIC) 3.0 guidance, and the CISA Cloud Security Technical Reference Architecture

In the short-term (0-2 years), all external entry points should be configured to support zero trust authentication. This closes the most commonly-used attack vector and meets the spirit of the CISA maturity model with the least amount of system impact. In the RFI outline, several systems were identified as day-1 targets:

- Okta Identity Cloud
- Cirrus Identity
- Azure AD
- Google Cloud Identity

Each of these systems would be configured to use BlockID as the Identity Provider (IDP) so they can have one authoritative source for strong proven identity. All four of these systems support standards-based authentication (SAML and OIDC) can be connected immediately, supporting the short-term deployment.

For more complex systems, integration via API and a connector called "Universal Web Login" allows a system to move to identity-based authentication with minor modifications. These connections should be part of a longer-term (2-4 year) strategy.

3. ZT implementation plan
    a. Identifies the assumptions and constraints the agency faces

The path to Zero Trust, especially the identity layer, can be done with a pragmatic and easily-achievable approach. Agencies are more resource-constrained than ever. That is why focusing on identity gives the largest benefit for the least effort. Furthermore, the user experience is actually improved as security is enhanced, which is a rare benefit offered by Zero Trust deployments.

    b. Identifies how the ZT roadmap would be implemented
    c. Addresses and prioritizes the risks the agency faces to implement its strategy and roadmap
    d. Discusses the impact to the agency's organizational and financial planning
    e. Includes how application programming interfaces (APIs), agents, and cloud services will be used

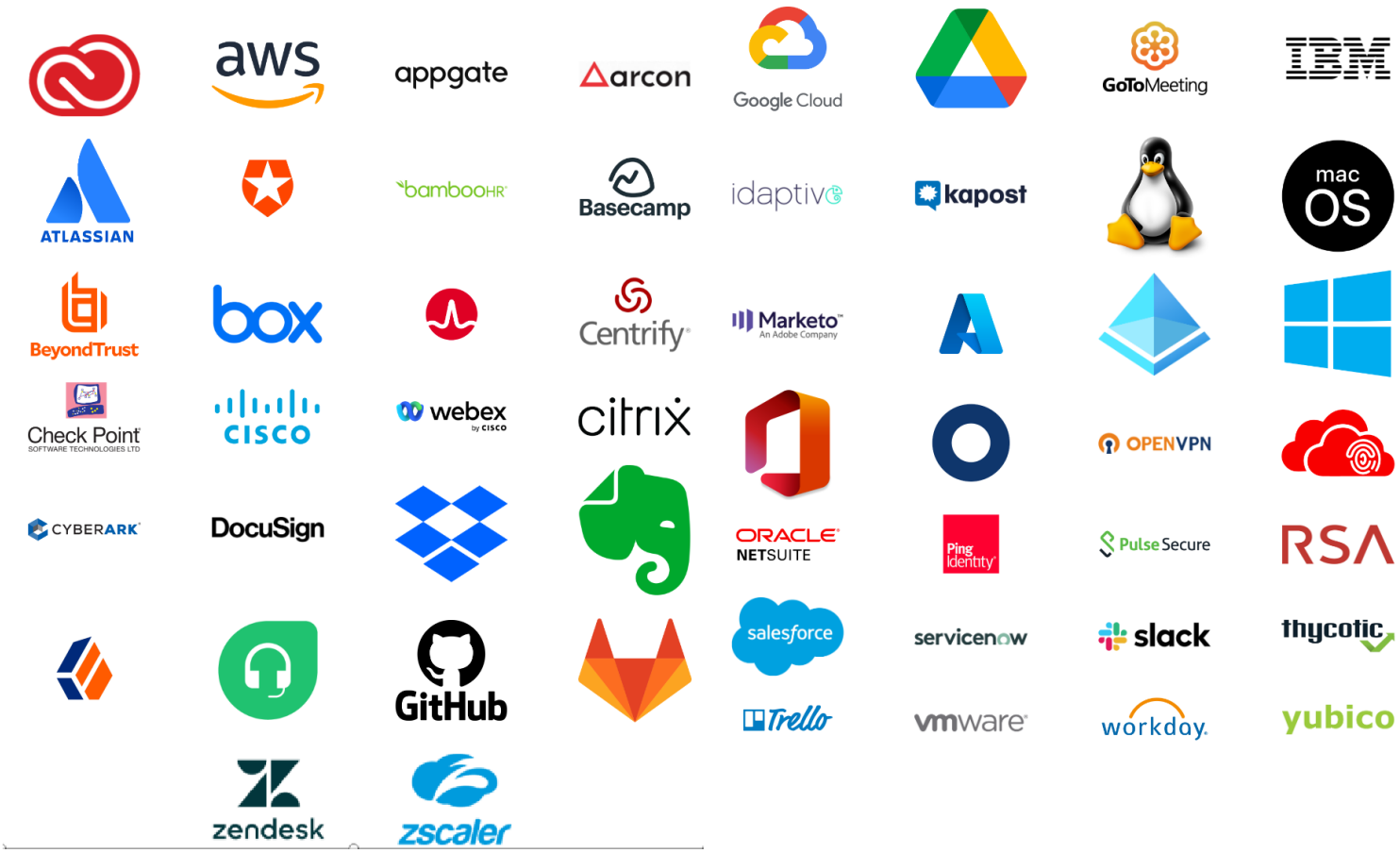
BlockID offers platform APIs through a next-gen developer experience. It allows for proofing, verification, passwordless, and integration APIs with a view to enhance interoperability and expand the addressable use cases.

Furthermore, a journey modeling tool offers a graphical editor for administrators to "put together any use case" they want to for passwordless authentication, authorization, federation, and identity proofing as well as NIST 800-63-3 identity verification.

A cloud-first deployment means agencies will not need to install and manage custom software, further simplifying the deployment.

The platform can also expand Windows Hello and MacOS authentication to include ecosystem devices such as Apple Watch and tablets and support for OAuth2 device flow for device onboarding and authentication.

Lastly, we offer integrations with over 150 target systems with out-of-the-box connectors. See this link and the image below for examples.



4. Impact on the organization's training needs
   a. What training is needed to implement the proposal by addressing both the technical staff and the users?

IT administrators will undergo a straightforward training process on how to connect BlockID to existing authentication systems to introduce zero trust. This only takes a few hours.

For end users, a focus on user-guided self-enrolment keeps the burden on IT to a minimum. However, to handle edge cases, user training videos can be leveraged to allow self-service for any exceptions.

b. Specific technical staff question: After receiving the required training, how long will it take a trained novice/apprentice network technician to become proficient in the effective installation, configuration, and operation of this proposed solution?

Less than 4 hours.

c. Specific user question: How much training will a user need to be able to support the anticipated changes (virtual private network [VPN], bring your own device [BYOD], installation of agents, etc.)?

We have deployed to millions of users with no formal training. The system was designed to be self-evident so the "steps to enable" are as simple as possible.

5. Total cost of operation
   a. Procurement and implementation costs

1Kosmos offers the Customer and Workforce module as a SaaS model. The subscription costs are normally prepaid annually. The "per user" list price is discounted further by volume and term. Based on the Client's needs, 1Kosmos may re-structure the invoicing, up to and including a "pay as you go" model in arrears to the actual adoption. If selected as the vendor or choice, 1Kosmos will build a plan that works for the agencies.

Given the guidelines of 60,000 total users and guidance of a $3m budget, 1Kosmos expects to be under budget for this project by over 30%.

b. Ongoing support and maintenance costs

The software is deployed as an annual "Software as a Service" (SaaS) model. There are no annual maintenance fees required to utilize the software other than the annual user licenses.

c. Proposed staffing plan that identifies the number and required expertise level for the operators of the proposed solution

The software is web-based and offers a self-evident administrative experience (AdminX). This allows any IT administrator that is proficient with existing software concepts to utilize it with no special training required other than several hours to get familiar with the capabilities and configuration concepts. A full-featured documentation portal and training videos allow operators to learn advanced configuration parameters over time at their own pace.

d. Potential for cost savings

There are 3 distinct ways that agencies can save money by adopting an identity-based authentication framework:

1. Reducing legacy 2FA and MFA systems - BlockID will replace legacy token-based and password-based systems with a flexible multi-faceted authentication framework. As each of these systems is replaced, the agency will recoup the hardware and software fees they typically incur.

2. The administrative burden will be greatly reduced, offering operational efficiencies. Because there will be one system to prove user identity, IT admins can focus on other system activities rather than managing dozens of different user frameworks.

3. The burden on the helpdesk can be reduced by 30% by offering millions in savings for medium-sized agencies. Once passwords are eliminated, there will be fewer calls. The savings are not only in helpdesk user time but also by allowing for staff efficiencies. A typical end-user spends hours each year dealing with forgotten passwords, broken authenticators, and other authentication challenges that can be eliminated.

6. User interface/user experience
   a. How will users be impacted by your proposal?

The user experience is enhanced, not reduced. By having one authoritative system for identity, there will be less confusion and faster response times for access.

7. Transferability to other agencies
   a. How might your proposal change if it were applied to a small or medium-sized agency?

Due to a cloud-first approach and self-user-directed deployment, it scales to any sized agency with the same, minimal amount of effort.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0650