Expanding the SIM Card Use Prize Challenge: Overview and Demo

Mike Bartock - NIST
Conor Patrick - SoloSim
Matt Lourie – Nok Nok Labs
Shane Weeden - IBM

#PSCR2020

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

*** Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change**

Agenda

- **Overview of the Prize Challenge**
- Hear from the Prize Challenge Winner
- Hear from two Creative Research and Development Agreement partners
- See a demo of the winning solution

SoloSIM

Conor Patrick

Founder, **SoloKeys**
@_conorpp

May 29, 2020

DISCLAIMER

This presentation was produced by guest speaker(s) and presented for publication in the National Institute of Standards and Technology's PSCR 2020: The Digital Experience. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government

Posted with Permission.

Finding out about SIM Card Challenge

+

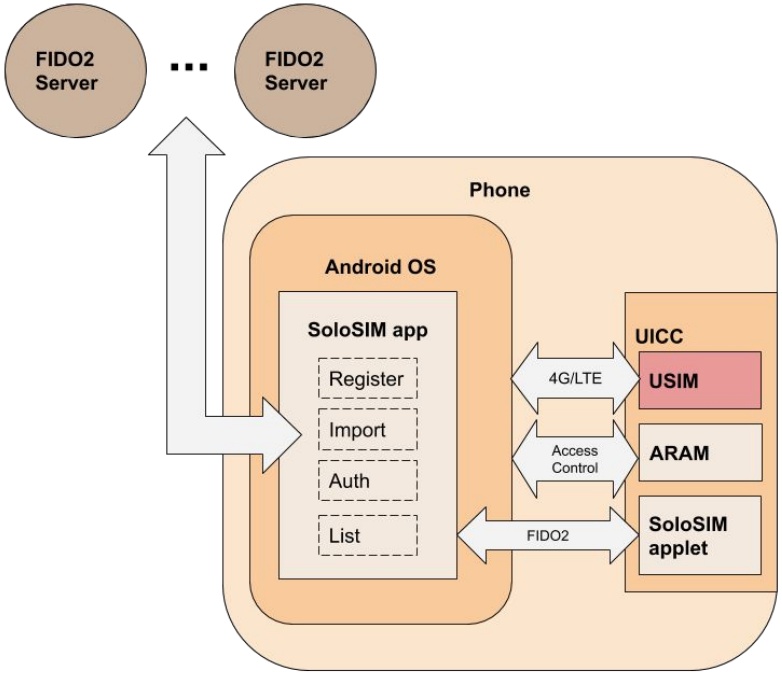
fido™

SoloKeys makes open source FIDO2 products, looking to expand open source platform (e.g. SIM card/smart cards).

Learned about SIM Card Challenge at HardwareCon.

Had a lot of FIDO2 authenticator knowledge, and learning about SIMs + solving authentication problems for a new market could be a great opportunity.

Designing the solution



ARAM is provisioned on UICC for Android OS to give SoloSIM access to UICC.

Overall design from the beginning.

App implements FIDO2 authenticator (CTAP) with SIM/UICC as a secure element.

App implements FIDO2 client + APIs to demo on multiple FIDO2 servers.

SIM Card

Biggest high level challenge is with the SIM card.

- Current SIM will not have “HSM” features to implement FIDO2.
- Political issue; not allowed to put custom apps on SIM.

Next best option for demonstration: **SIM overlay**.

Development challenges

Android restricts access to SIM card.

- SIM card needs to have a standard set of “access rules” installed
  - Tells Android what signed apps are allowed to interact.
- Debugging required building and installing custom Android ROMs.

(**iOS** likely has similar API + restrictions, but it is undocumented).

FIDO2 interoperability. Many cryptographic elements and types of encodings at play. Difficult to see & figure out what is wrong.

- Thankfully the transport binding API was used for both IBM & NokNok

Overall experience

- Great challenge
  - Developing flexible/mobile/interoperating root of trust is a much needed solution
  - Opportunity provided by NIST PSCR went very well overall

- Work is ongoing
  - Still restrictions with using with SIM cards.
    - Makes bottom-up/startup approaches difficult.
  - **Short term**:
    - SoloSIM (now “Authim”) now focusing on evidence authenticity app solution.
  - **Long term**:
    - SoloKeys focusing more making an open platform for smart cards.
      - Making an open & Global Platform compliant device that can run applets.
      - Open USIM + eSIM apps.

Use of funds

$37.5k awarded, $4k of which is for business development.

~ $3k

- Coworking space
- Travel costs; Going to CES
- Incorporation fees
- More phones for testing + development

~ $5k

- Reinvesting in new IP (evidence authenticity app for first responders).
    - Funding development
    - Teamed up with another developer
    - Make automatic way to take evidence + using root of trust on phone.

Thank you!

If you have any questions, please email me directly at conor@solokeys.com

The Trusted Leader in Passwordless Authentication

Matt Lourie
Sr. Director of Engineering

DISCLAIMER

This presentation was produced by guest speaker(s) and presented for publication in the National Institute of Standards and Technology's PSCR 2020: The Digital Experience. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government

Posted with Permission.

Agenda

- About Nok Nok
- S3 Authentication Platform
- How Contestants used Authentication Service

nok nok

Who is Nok Nok?

- **Deep domain expertise in FIDO next-generation authentication**
  - We invented FIDO (ex-PGP team)
  - Experts in Consumer Authentication

- **Most widely deployed B-to-C passwordless solution**
  - 200M+ Users
  - Billions of authentications

- **Proven technology with innovations based on the real world**
  - Servers deployed globally at scale
  - More than 90 US- and International patents issued or filed

Simple, Strong, Scalable
Any App, Any Device, Any Authenticator

nok nok

NIST / Nok Nok Partnership

- Bill Fisher (NIST) introduced Nok Nok to NIST in 2014
- Nok Nok collaborated with National Cybersecurity Center of Excellence (NCCoE) on Mobile Single Sign On using FIDO
- Nok Nok solution for First Responders highlighted in NIST Webinar in 2017
- Nok Nok has deep knowledge of authentication needs of Public Safety communication solutions

nok nok

Why FIDO?

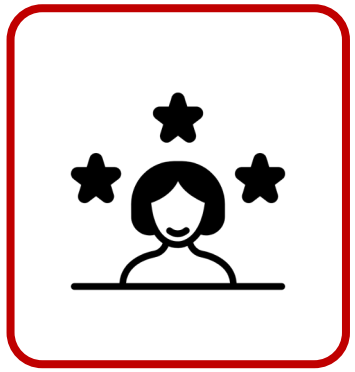
- **Industry Standard**
  - Interoperable, secure approach
  - Certification program for compliance
  - Global standard supporting regulatory requirements, e.g. PSD2 SCA, eIDAS
- **Secure**
  - No shared secrets
  - Leverages public key cryptography
- **Privacy Preserving**
  - Only public keys stored on server
- **Cost Effective**
  - Reduced operational complexity and costs

Combine optimal security with optimal convenience

nok nok

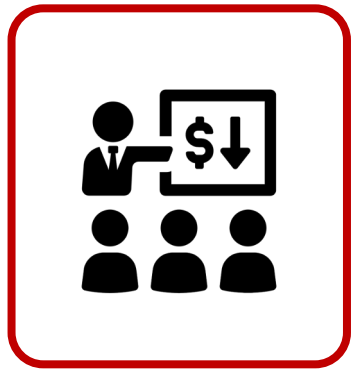
Nok Nok Delivers Many Business Advantages

Improve Customer Experience



- Improve onboarding success rate
- Improve authentication speed
- Reduce transaction abandonment

Reduce Costs



- Reduce call center costs due to password resets
- Reduce SMS OTP costs
- Reduce development costs to support MFA

Meet Regulatory Requirements and Reduce Fraud

- Meet PSD2 SCA requirements
- Reduce ATO
- Reduce phishing attacks
- Reduce man-in-the-middle attacks

nok nok

Global Brands Trust Nok Nok for Their Solution

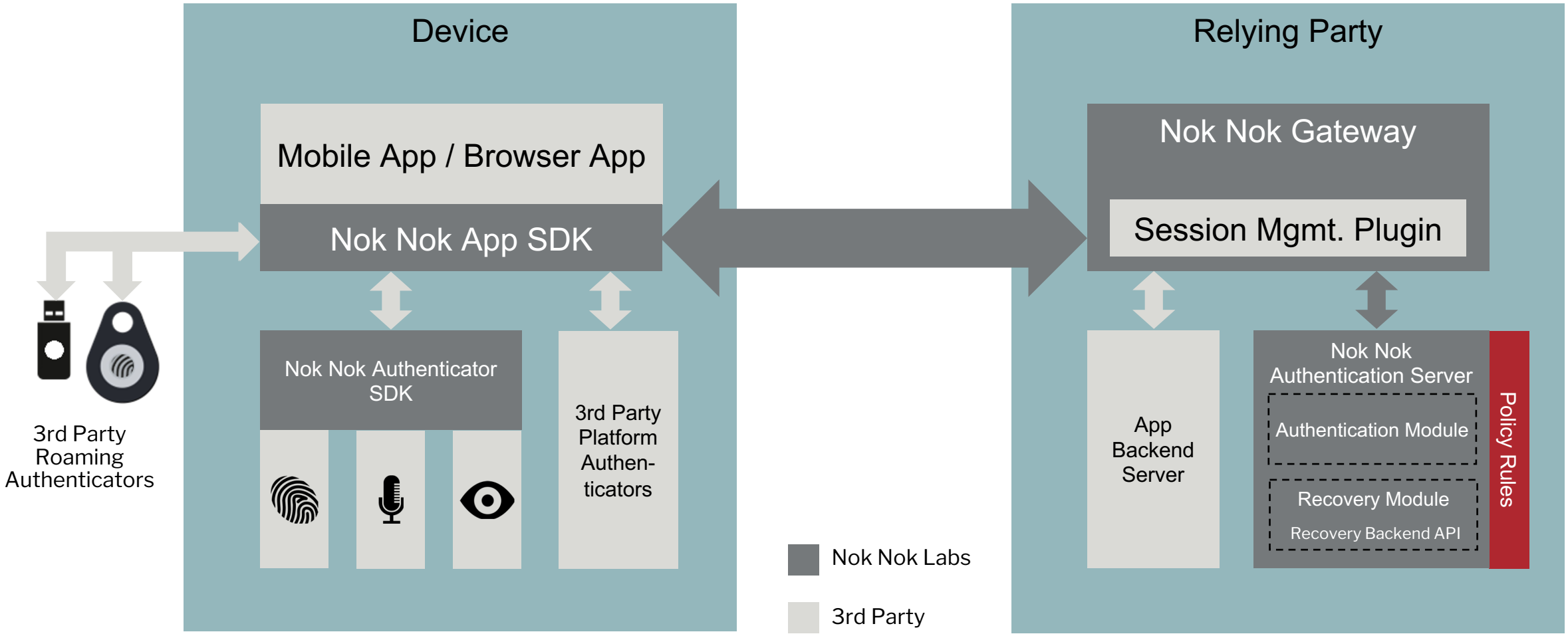
4 industry leading Financial Services Firms

4 out of 5 of the world's largest banks

4 major Mobile Network Operators (MNOs)

Global Partners Rely on Nok Nok for Authentication

S3 Authentication Suite Architecture

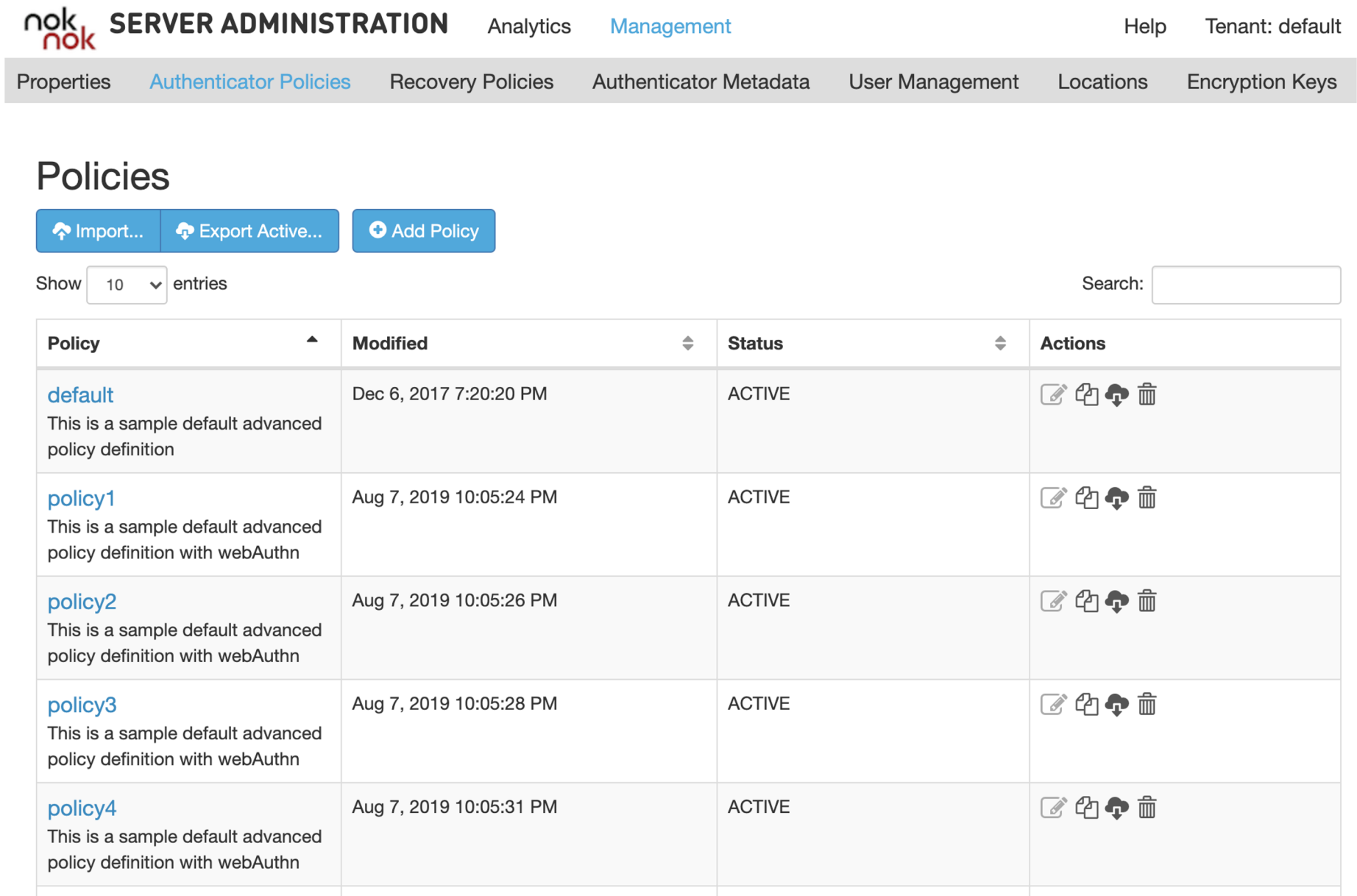


Contestant Setup using Cloud Service

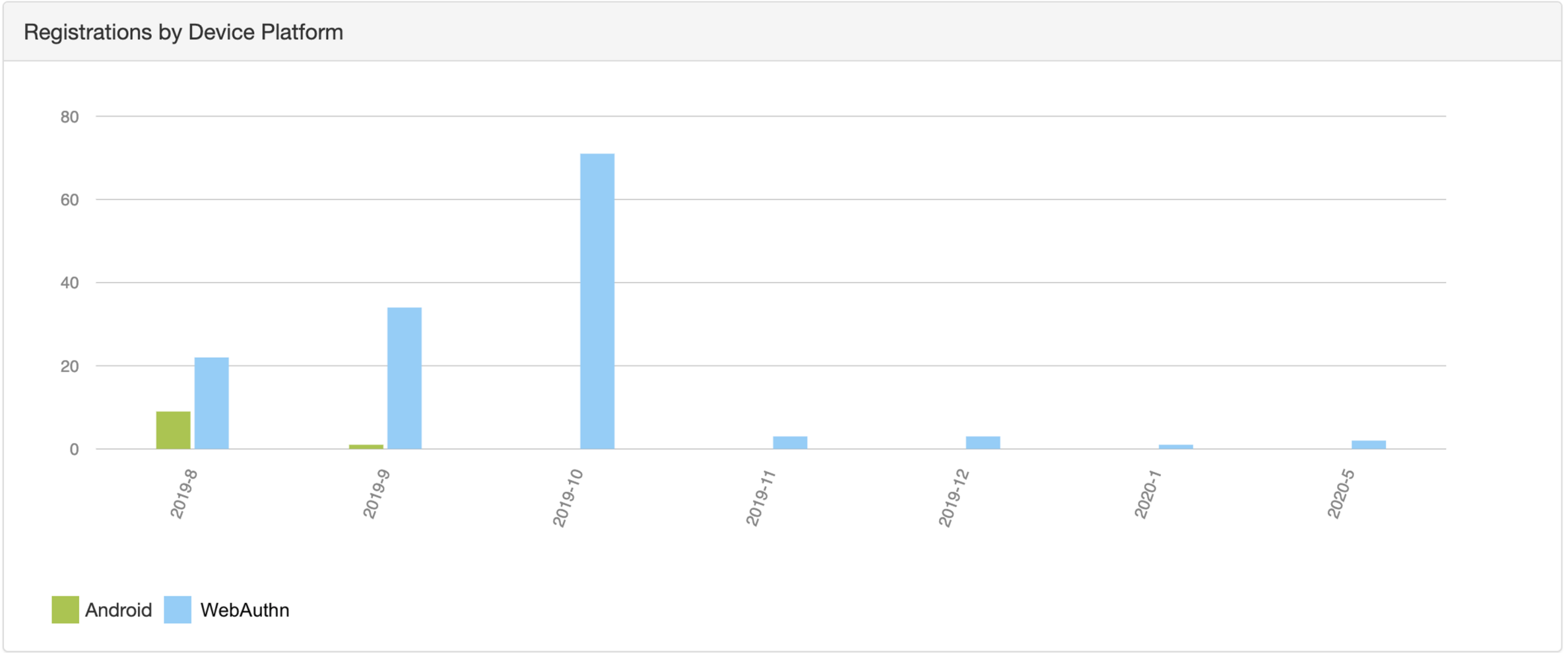
- Product supports both on-premise and cloud deployment
- For simplicity, contestants were set up in the cloud
- Contestants used REST API Integration
- Federation Connectors are also supported

nok nok

Administration – Authenticator Policies



Administration – Analytics



Contestant Administration: Drill Down

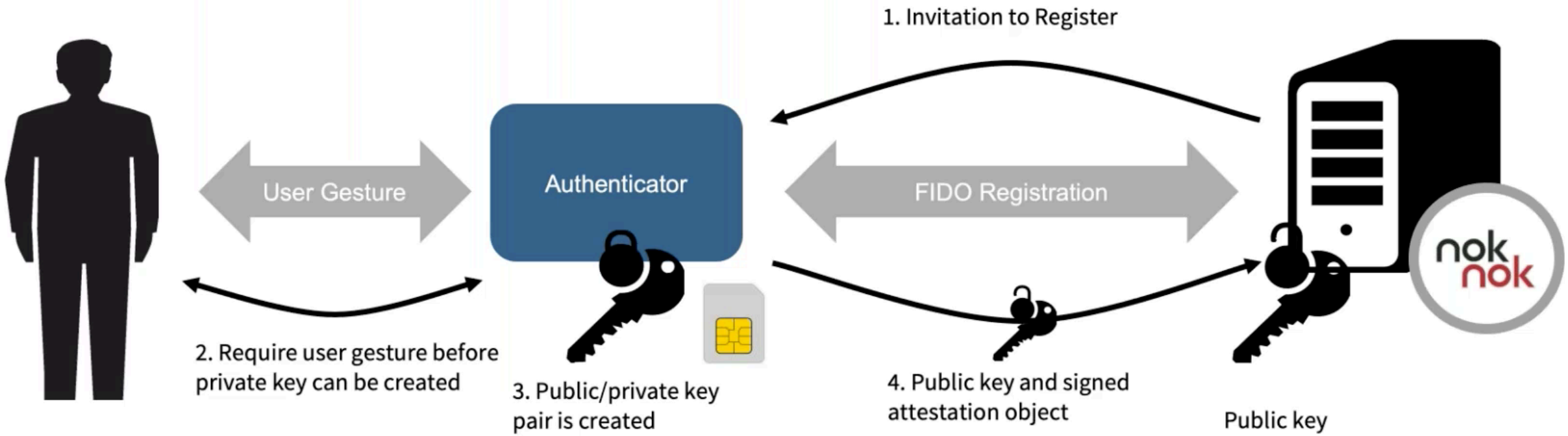
Authentication

ID	Device Name	Device Model[?]	OS	Manufacturer	Authenticator	Authenticator Description	Timestamp	Country	Status Code
abcdef12345ghijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a-11e9-9cb5-2a2ae2dbcce4	solokeys_user	12/3/2019, 8:16:17 AM	Unknown	OK
abcdef12345ghijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a-11e9-9cb5-2a2ae2dbcce4	solokeys_user	12/10/2019, 7:33:46 AM	Unknown	OK
abcdef12345ghijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a-11e9-9cb5-2a2ae2dbcce4	solokeys_user	1/8/2020, 11:37:59 AM	Unknown	OK
abcdef12345ghijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a-11e9-9cb5-2a2ae2dbcce4	solokeys_user	1/8/2020, 10:11:36 AM	Unknown	OK
abcdef12345ghijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a-11e9-9cb5-2a2ae2dbcce4	solokeys_user	12/2/2019, 12:16:41 PM	Unknown	OK

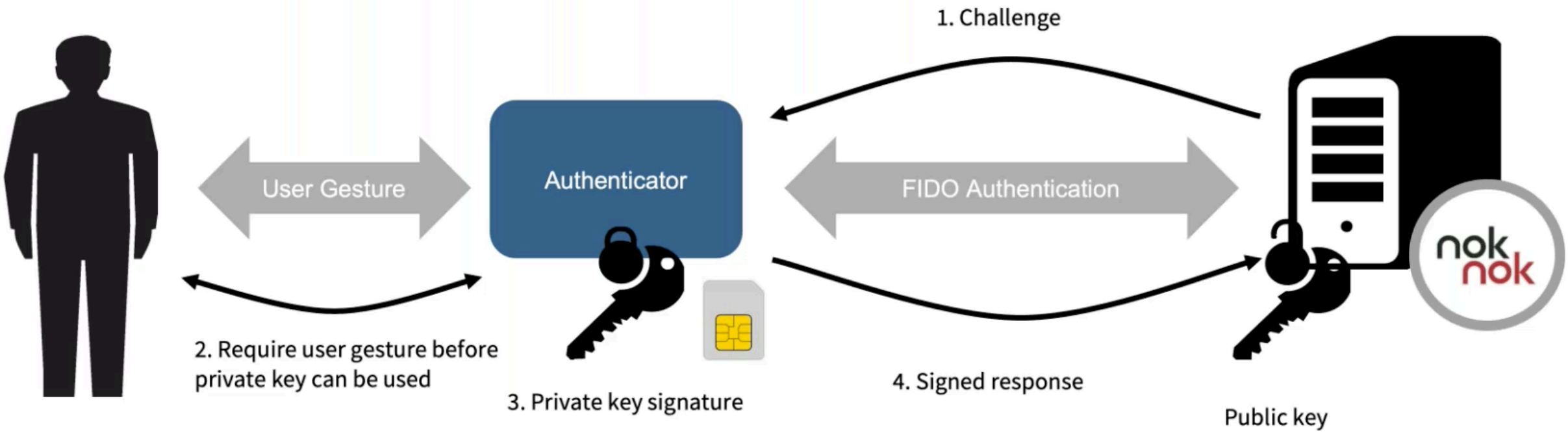
More

nok nok

FIDO Registration with SIM Card



FIDO Authentication with SIM Card



THANK YOU

IBM Security - industry outreach with NIST

Expanding the SIM Card Use for Public Safety

PSCR

NIST

Shane Weeden
Senior Technical Staff Member

IBM **Security**

IBM

DISCLAIMER

This presentation was produced by guest speaker(s) and presented for publication in the National Institute of Standards and Technology's PSCR 2020: The Digital Experience. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government

Posted with Permission.

Unified security for a hybrid multicloud world

Hundreds of open integrations at the center of your ecosystem

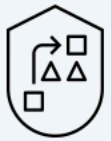
Recent Highlights

OPEN CYBERSECURITY ALLIANCE

CISCO

Red Hat

The industry's broadest and most complete security portfolio



Strategy and Risk

Advance Security Maturity
- Strategy and Planning
- Risk Assessments
- Advisory Services

Build Leadership and Culture
- IBM Security Command Center
- IBM Security Command Mobile
- IBM Security Command Onsite
- IBM Security Command Virtual

Threat Management

Stop Advanced Threats
- Security Operations Consulting
- X-Force Threat Management Services
- X-Force Red
- QRadar

Orchestrate Incident Response
- Resilient
- X-Force IRIS

Master Threat Hunting
- i2 Intelligence Analysis
- QRadar Advisor with Watson

Digital Trust

Protect Critical Assets
- SDLC Consulting
- Data Protection Services
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager

Deliver Digital Identity Trust
- Trusteer
- Verify

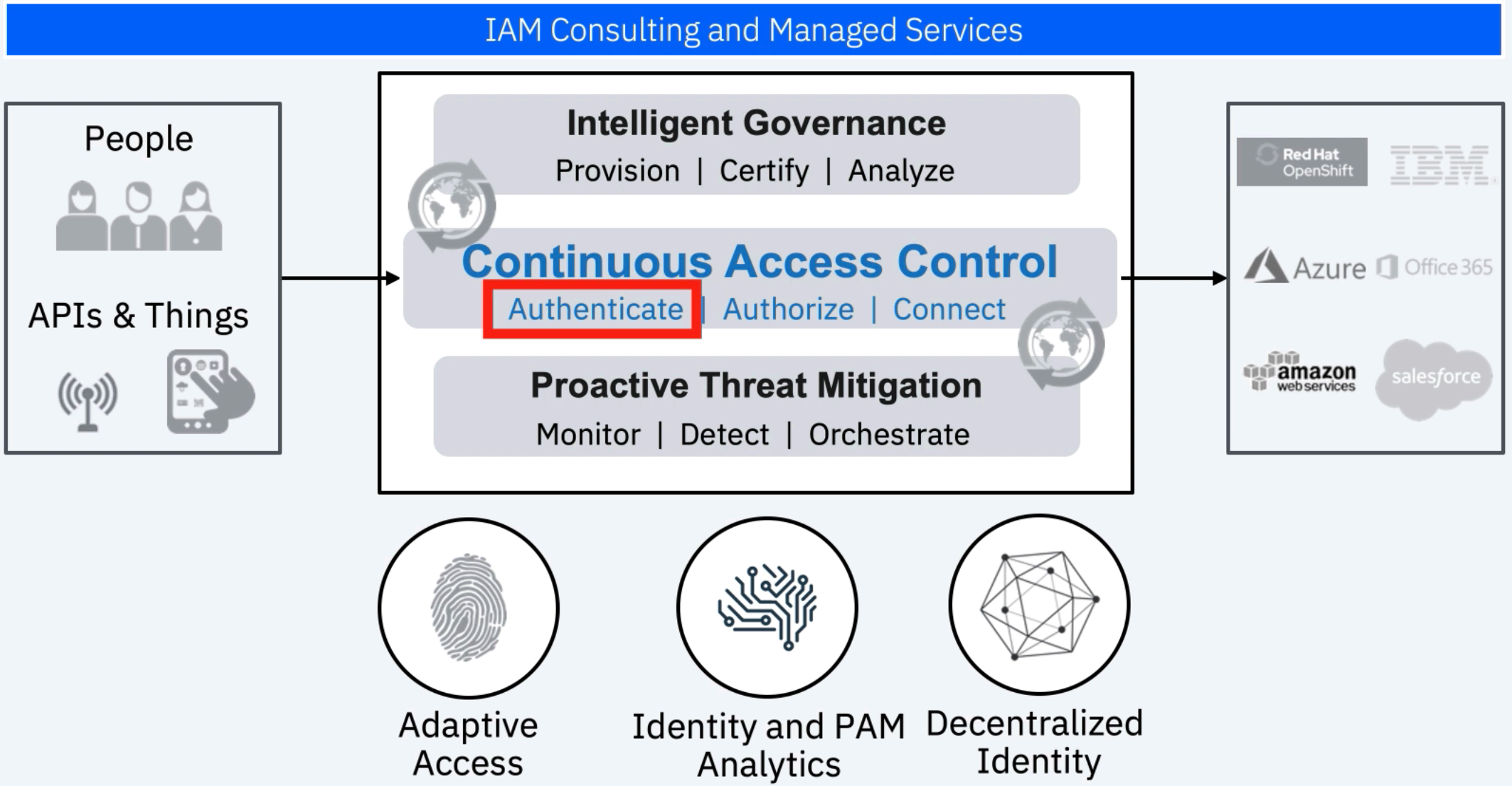
Govern Users and Identities
- Identity Management Services
- Identity Governance
- Verify
- Verify Access
- Secret Server

Unify Endpoint Management
- Endpoint Management Services
- MaaS360

Secure the journey to cloud Cloud Pak for Security | Cloud Security Services | Cloud Security Products

Smart Identity for the Hybrid Multicloud World

Securely connecting every user, API, and device to every app in and outside the enterprise



IBM Security Verify: Smart Identity for the Hybrid Multicloud World

Serving both workforce and consumer populations

Single Sign On (SSO): One-click access
Eliminate password hassles with a unified application launch pad and SSO from any device, to any cloud or on-premises application

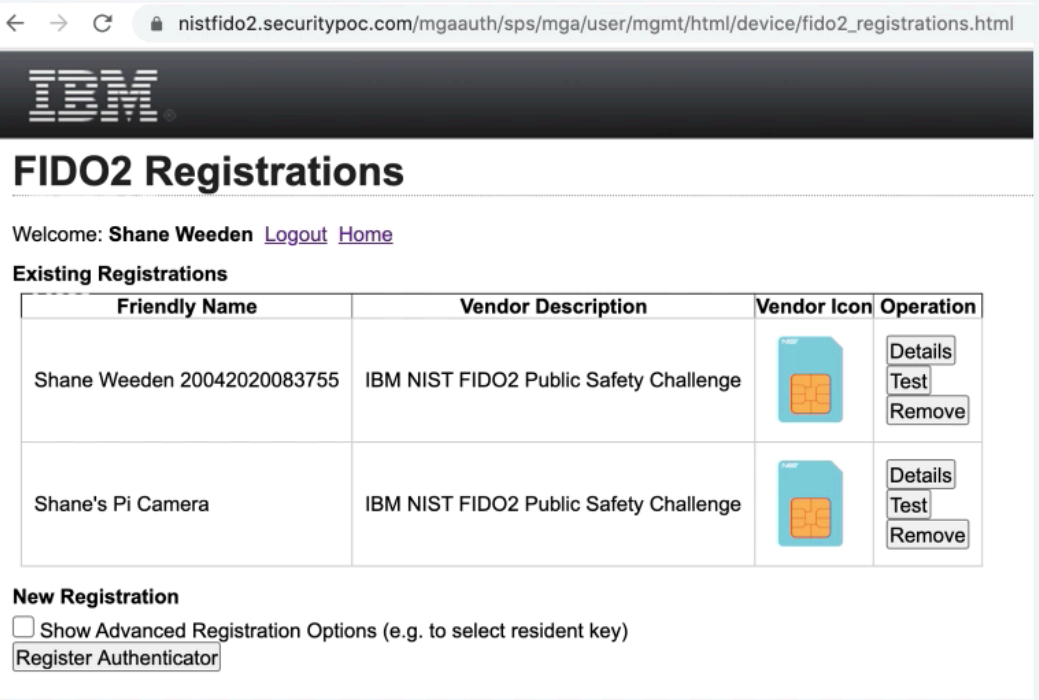
Multi Factor Authentication (MFA): 2FA to any target system
Protect web, cloud, mobile, VPNs, and operating systems with a common platform for MFA, including passwordless technologies such as FIDO2

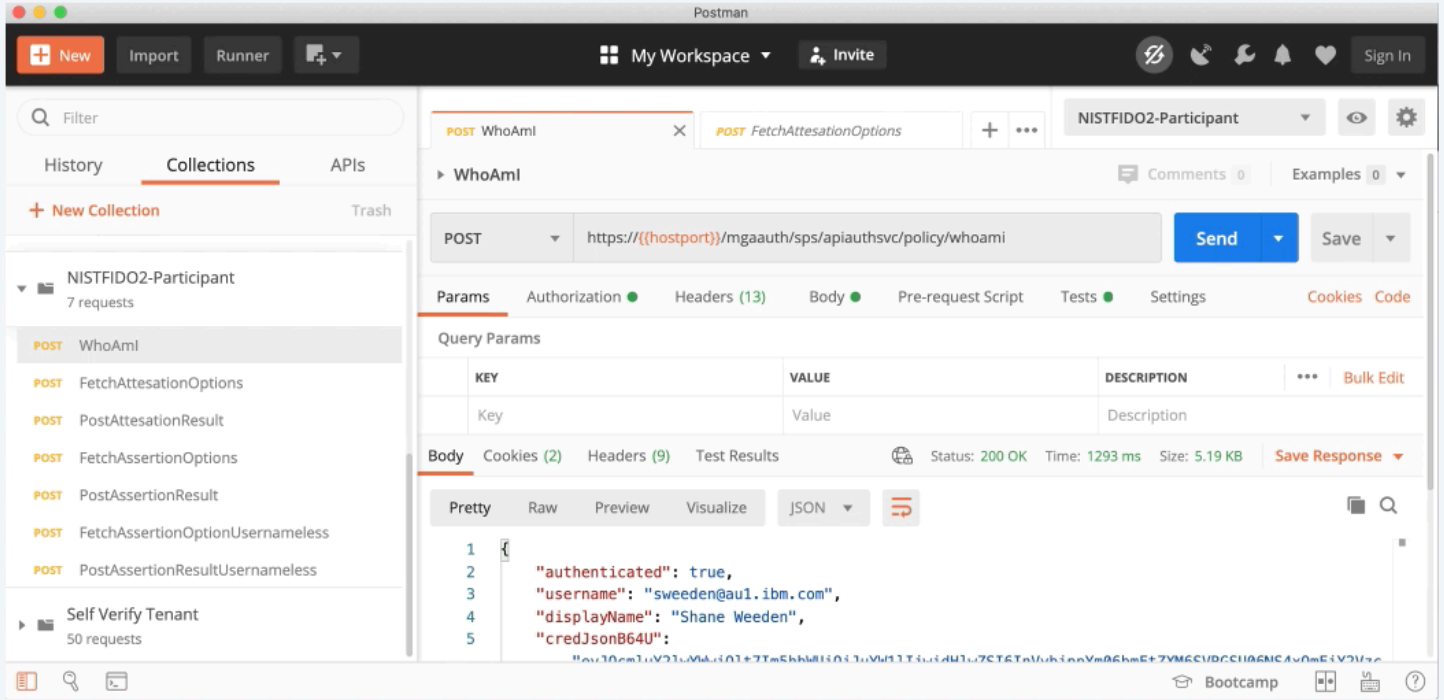
Governance: User lifecycle management and compliance
Request, approve, provision, and periodically recertify user access to applications

Adaptive Access: Balance security and convenience
Dynamically assess full user, device, and environment context for an AI-powered, aggregated risk score, and enforce MFA when risk is high

Analytics: Mitigate identity-related risks through a holistic view of IAM data
Process activity and entitlement data from a variety of sources, providing a 360 view of access risks with the ability to take action based on those risk insights

Supporting NIST participants with IBM Security Verify Access





- Simple easy-to-use web portal for viewing and managing FIDO2 registrations.
- Downloadable POSTMAN collection (and instructional video) containing a complete JavaScript implementation of a FIDO2 client.

Participants need only implement the algorithms available from the POSTMAN collection in their mobile phone application.

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM

References:

- https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/past-prize-challenges/2019-expanding-sim-card-use-public
- https://solokeys.com/
- https://noknok.com/
- https://www.ibm.com/blogs/sweeden/cloud-identity-fido2-consuming-fido2-as-a-service-from-ibm-cloud-identity/

THANK YOU