

RSAConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: **PART4-W02**

Digital Trust & Cybersecurity 2025: A Call for Openness & Interoperability

David Mahdi

CSO & CISO Advisor
Sectigo

TRANSFORM



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 LLC 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.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

RSA[®]Conference2022

Part 1: Digital Trust & Cybersecurity



RSA®Conference2022

Part 1: Digital Trust & Cybersecurity

Digital Trust is an Outcome of Cybersecurity



It's All About Digital Trust

Gartner®



WORLD
ECONOMIC
FORUM

Deloitte.

Draft NIST Special Publication 800-160, Volume 1
Revision 1

Engineering Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
MARK WINSTEAD

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-160v1r1-draft>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

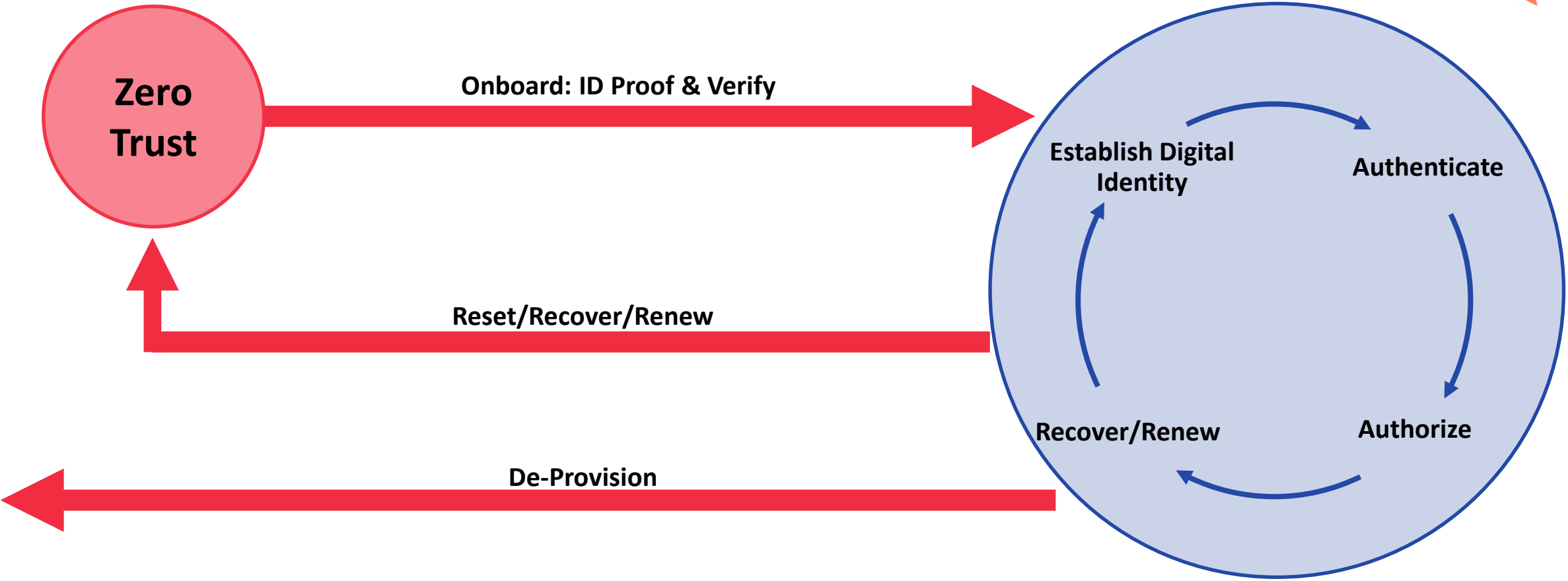
Digital Trust & Zero Trust: Incompatible?



Sorry – We Need Trust!



Goal: Establish & Maintain Trust



Digital Trust Architecture

Digital Business

Digital Trust

Digital Identities:

Humans | Apps | Cloud | Devices | Machines

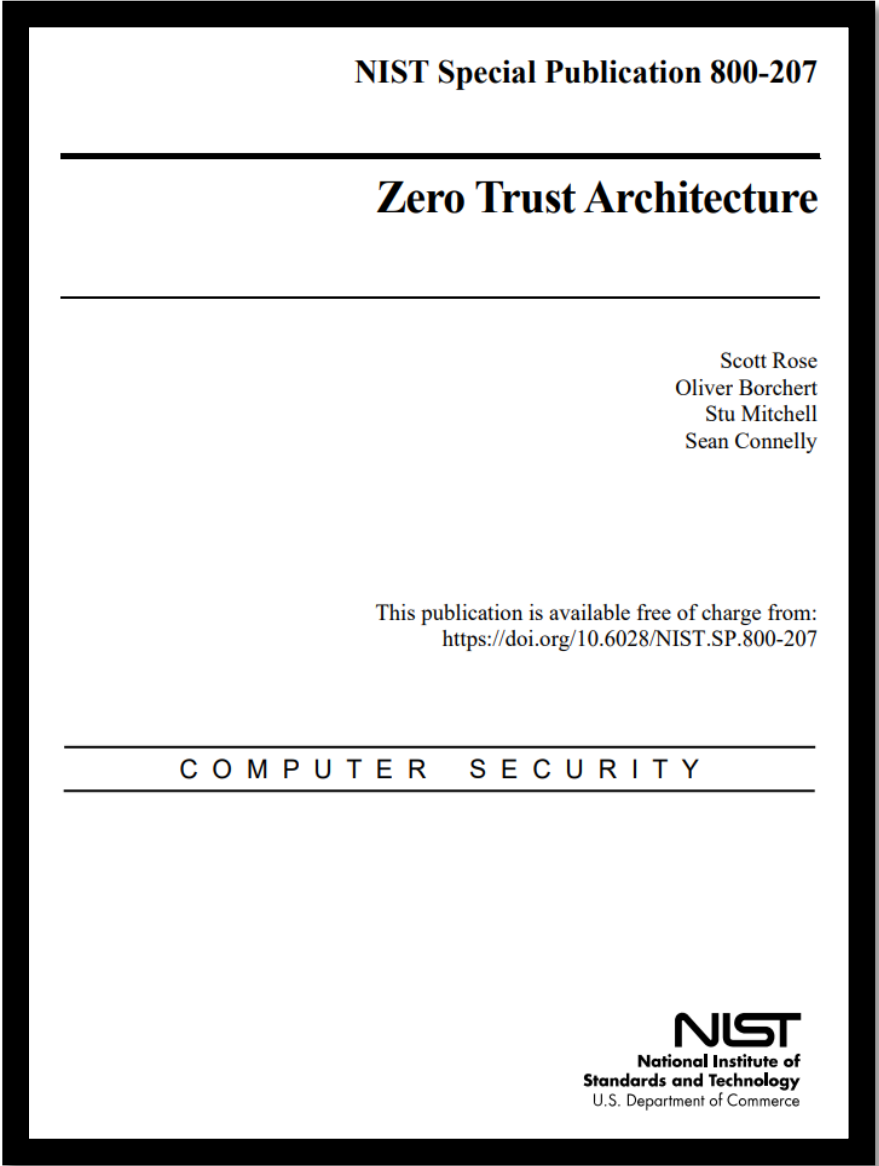
Data:

Structured | Unstructured | Semi-Structured

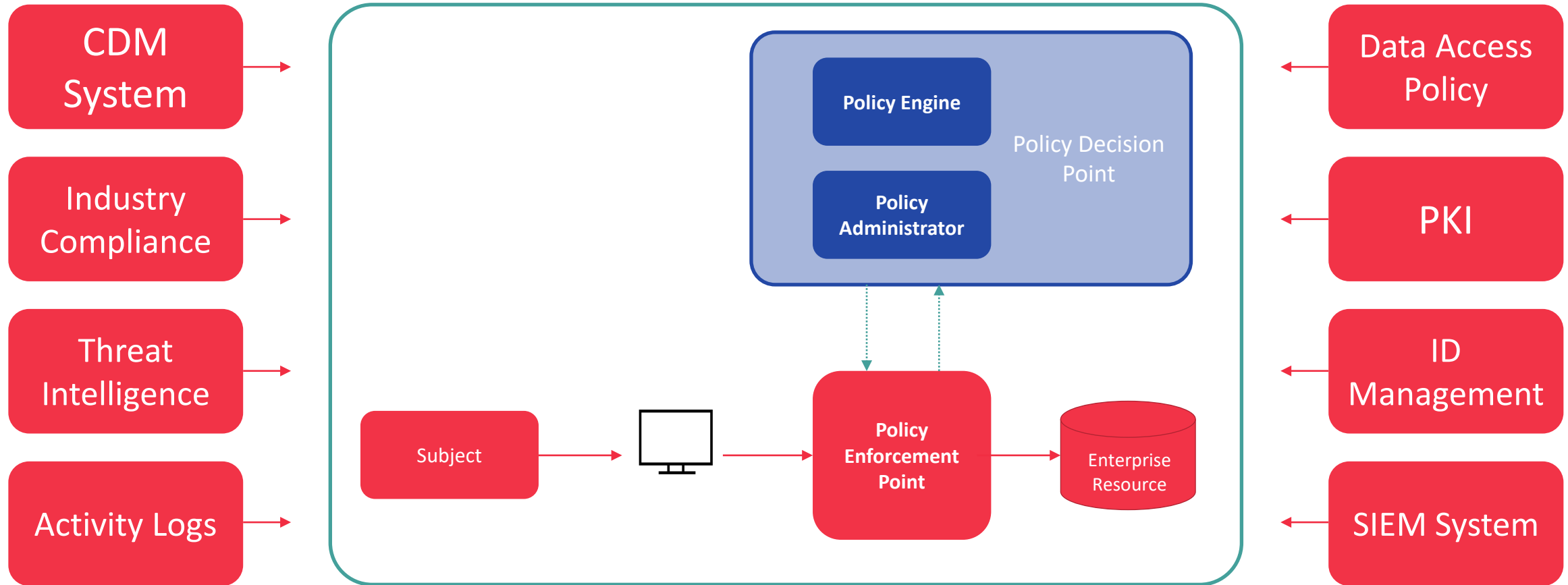
Rooted in Cryptography

Keys | Certificates | Secrets

NIST 800-207: Zero Trust Architecture



NIST Zero Trust Architecture



Source: NIST Zero Trust Architecture SP 800-207

NIST 800-207: Identity-First Security

**NIST Zero Trust Architecture
[SP 800-207] calls out...**



**ID Management
(also known as IAM)**



**Public Key Infrastructure
(PKI)**

WHY?

Digital Trust Architecture

Digital Business

Digital Trust

Digital Identities:

Humans | Apps | Cloud | Devices | Machines

Data:

Structured | Unstructured | Semi-Structured

Rooted in Cryptography

Keys | Certificates | Secrets

Identity Management: Focuses on Humans....



Access Management

SSO



Privileged Account Management

Cloud Infrastructure Entitlements Management (CIEM)



Identity Governance & Administration (IGA)



User Authentication

- Passwordless authentication
- Biometrics
- Mobile

**IAM = \$25B Market
by 2025**

Source: Gartner, Markets & Markets

But What About Non-Humans?

- **68%** of non-humans or bots have access to sensitive data and assets.
- **Machine identities** now outweigh human identities by a factor of 45x on average.

Machines Are Already Here!

Source: CyberArk [CyberArk Report: Massive Growth of Digital Identities Is Driving Rise in Cybersecurity Debt](#) | CyberArk

Non-Humans: Machine Identities

- What Are Machine Identities?
- Devices
 - IoT/OT, Mobile, Laptops/Desktops
- Software & Apps
 - Workloads, Containers, VMs
- Robotic Process Automation
 - Bots
 - Supervised and/or Unsupervised

**Machine Identity
Management:
Top Security & Risk
Trend (Gartner)**

Digital Trust Requires a Harmony of Humans and Machines



Digital Identities:

Humans | Apps | Cloud | Devices | Machines

Data:

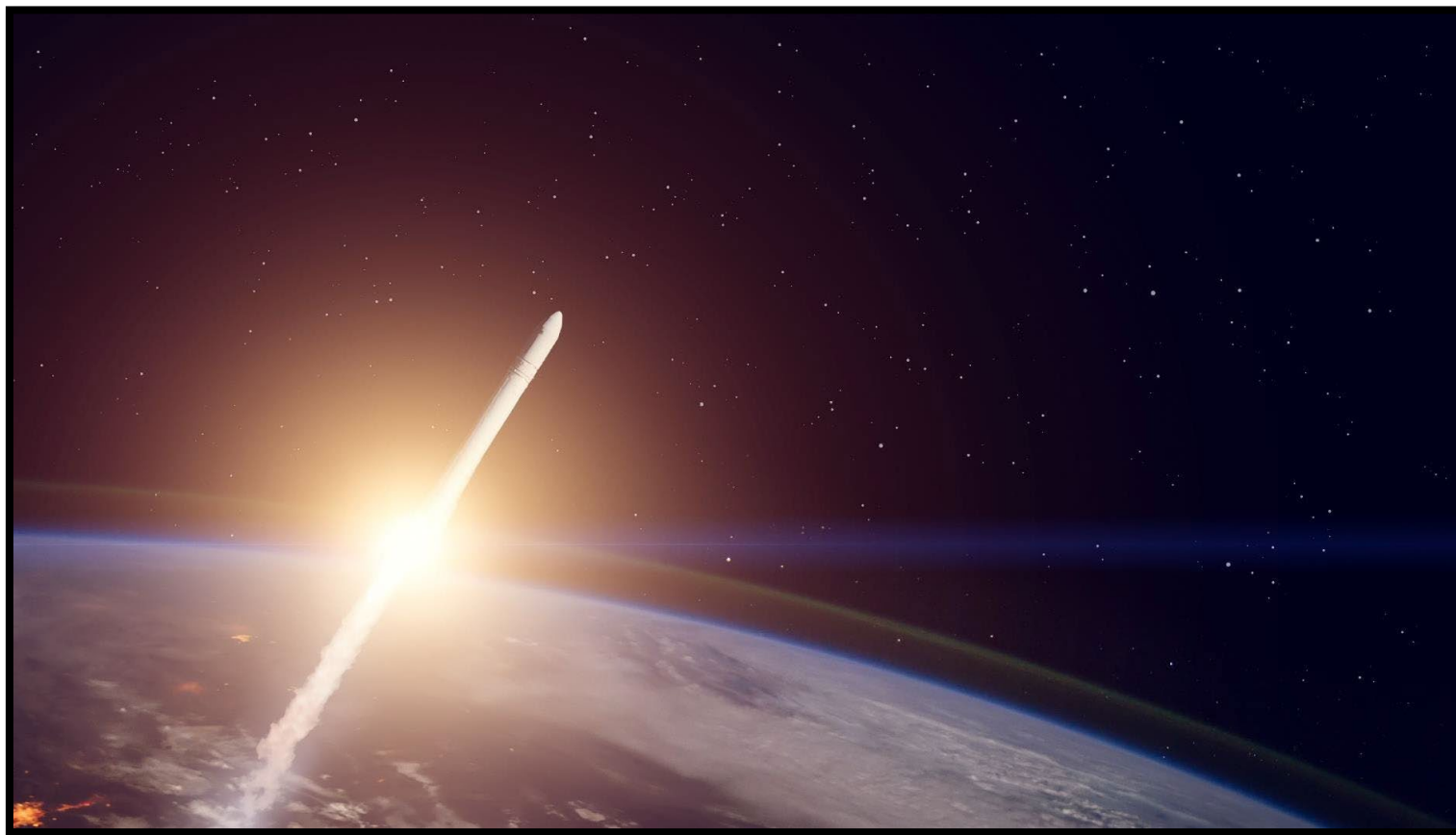
Structured | Unstructured | Semi-Structured

Identity-First Security: Platform for Human & Machine Identities

Rooted in Cryptography

Keys | Certificates | Secrets

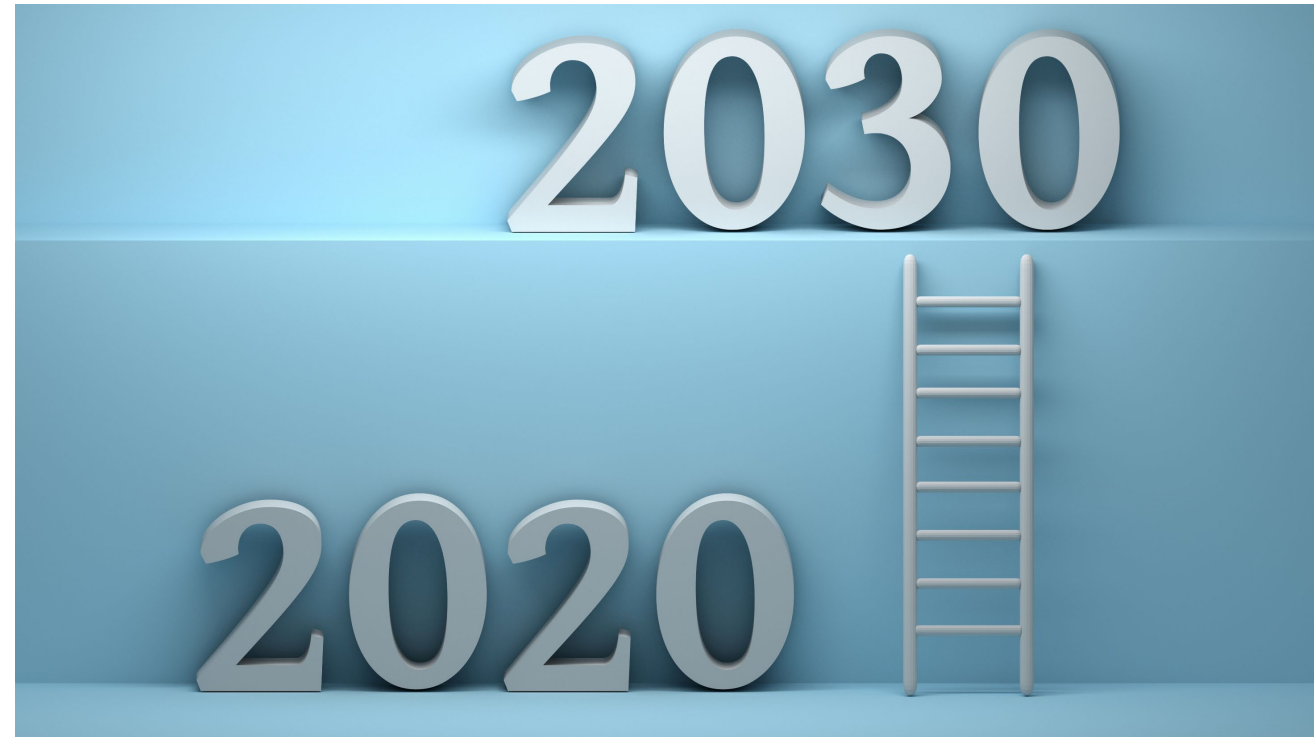
2022 Is the Year of PKI!



PKI is the Technology for the 2020's

Fun Fact...

- Did you know that PKI underpins Blockchain & Web 3.0 ?



Back to the ~~Past~~ Future with PKI

Public
Web

Private:
Machine
Identities

- Code
- Intranet
- Servers
- Bots

Passwordless
Authentication

IoT Security
Device
Identity

Document
Signing

Zero Trust
Network
Architecture

Digital
Trust....

PKI | Keys | Secrets | Crypto

COAR: Cryptography Orchestration, Automation & Response

Identity-First Security: Platform for Human & Machine Identities

“Apply”



- **Digital Trust is the Outcome of Great Cybersecurity!**
- **Zero Trust is important but...Establish and Maintain Digital Trust**
 - Focus on Identity First Security
- **Digital Trust – Requires Harmony of Humans & Machines**
- **PKI @ the Core of Human and Machine Identity**
 - PKI and CLM is here to unite use cases
 - Explore ways where you can expand your use of PKI-based methods
 - Areas:
 - Passwordless, Device Auth, DevOps, Document Signing, ZTNA, and so on.

RSA®Conference2022

Part 2: A Call for Openness & Interoperability

Digital Trust & Cybersecurity products and services must work together!



The Digital World

- Metaverse
- AR / VR
- Connected Future...



Well, Not if Things Don't Work Well together!



Bluetooth – It Just Works...Well Kind of... 😊



Imagine a World Without Bluetooth?!

It would be a mess of drivers and software

Let's not talk about dongles?!



Well, That is The Case for Digital Trust and Cybersecurity



- Crypto & PKI
- Key Management
- Blockchain Platforms
 - Identity Wallets
 - NFTs
 - Web 3.0



CISOs & Teams Are Managing Too Many Security Products

- SWG | SASE | ZTNA
- EPP | EMM | SIEM
- EKM | SSL/TLS | CLM
- DLP | DAG | CASB
- Authn | Authz | AM



Cybersecurity Product & Vendor Consolidation

- **78%** of CISOs have 16 or more tools in their vendor portfolio
- **80%** of CISOs want to consolidate & have plans for vendor/product consolidation
 - Sometimes sacrificing capabilities; trading for ease of management and orchestration

“For CISOs, CIOs and their teams to be successful, they can’t rely on a ton of security products just to function. It simply isn’t sustainable.”

Source: [Gartner Top Security and Risk Trends](#)

A Perfect Storm



We Need Openness & Interoperability



What is Openness & Interoperability, and What does it Mean for Cybersecurity, and Digital Trust

What is Openness?

- Publishing APIs
- Embracing Ecosystems & Communities
- Working with overlapping products & solutions
- Coexisting with others



Security Vendors Cannot Be Islands Anymore!

What is Interoperability?

E.g., Identity First, PKI & Digital Trust Standards:



EST

{REST:API}



SCEP



ENABLED

CSC API



CLOUD
SIGNATURE
CONSORTIUM



ACME

- Acme logo: https://en.wikipedia.org/wiki/Automatic_Certificate_Management_Environment
- S/MIME logo: <https://seeklogo.com/vector-logo/121116/s-mime-enabled>
- eID.AS logo: <https://www.eid.as/>

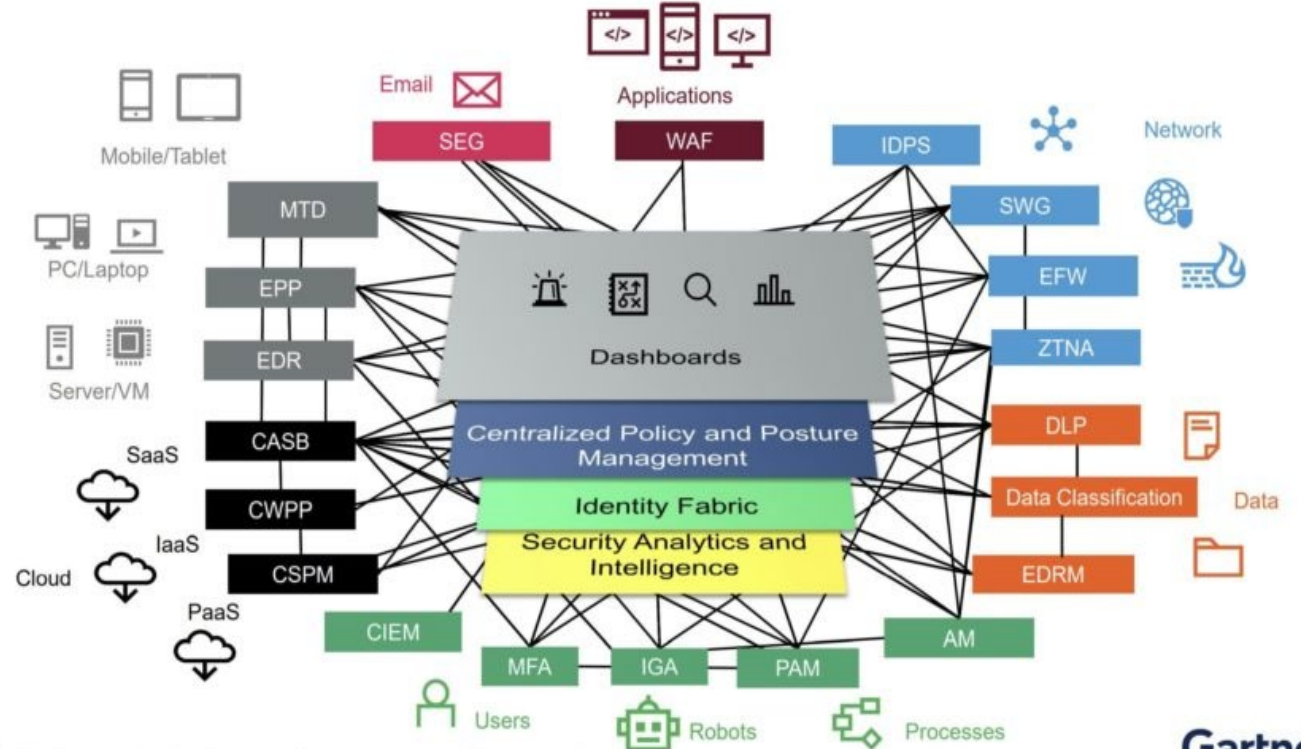
There is Hope!



Gartner Cybersecurity Mesh Architecture (CSMA)

- Top Strategic Security and Risk Trend, 2021, 2022
- New Paradigm for cybersecurity
- Distributed, Scale, Flexibility and Control
- Standards and Interoperability at the Core

Cybersecurity Mesh Architecture Complete



Security standards (Source: Gartner) & [Cybersecurity Mesh and Decentralized Identity Explained \(esecurityplanet.com\)](https://www.esecurityplanet.com/cybersecurity-mesh-and-decentralized-identity-explained/)

Gartner CSMA: Standards & Interoperability

- Threat Detection: STIX/TAXII, SIGMA
- IAM: SAML, Oauth, SCIM, XACML, OPA, JWT
- Network Format: Ipfix
- Nascent: IDQL, CAEP
- Other: OpenDXL, NIST SCAP v2
- Standard Formats: Snort, ZEEK, Yara (Language)
- Framework: OWASP Top 10, MITRE [ATT&CK / D3FEND], CVSS, Cyber Kill Chain, CVE

Security standards (Source: Gartner) & [Cybersecurity Mesh and Decentralized Identity Explained \(esecurityplanet.com\)](https://www.esecurityplanet.com/cybersecurity-mesh-and-decentralized-identity-explained/)

Gartner CSMA: Strategic Planning Assumption

“By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%.”

Source: Gartner & [Fortinet Security Fabric: The Industry's Highest-performing Cybersecurity Mesh Platform](#)

A Call to Digital Trust Market Participants



IAM Providers Need to
Work Together



Document Signing and Signatures



Device Manufacturers



Key, Secret & Certificate Managers



Certificate Authorities
Must Embrace a CA
Agnostic Approach



Cloud Service Providers

“Apply”

- **Default to Interoperability**
 - By way of standards vs. proprietary agents and methods
- **Familiarize yourself with Gartner’s CSMA**
- **Get to know current and emerging standards**
 - ACME, CSC API, EST
- **When renewing or buying new security products**
 - Pressure vendors to use open standards
 - Mitigate risk by deemphasizing proprietary heavy solutions

RSA®Conference2022

Thank you!

