MIT Kerberos & Internet Trust Consortium

Mission & Vision

May 2014

MIT KIT INTERNET TRUST

Contents

- Brief History
- MIT-KIT Mission
- Emerging Personal Data Ecosystem
- MIT-KIT Projects
- Advisory Board & Academic Board
- Membership & Benefits

MIT KIT INTERNET TRUST

Brief History

Kerberos: 1987 - today

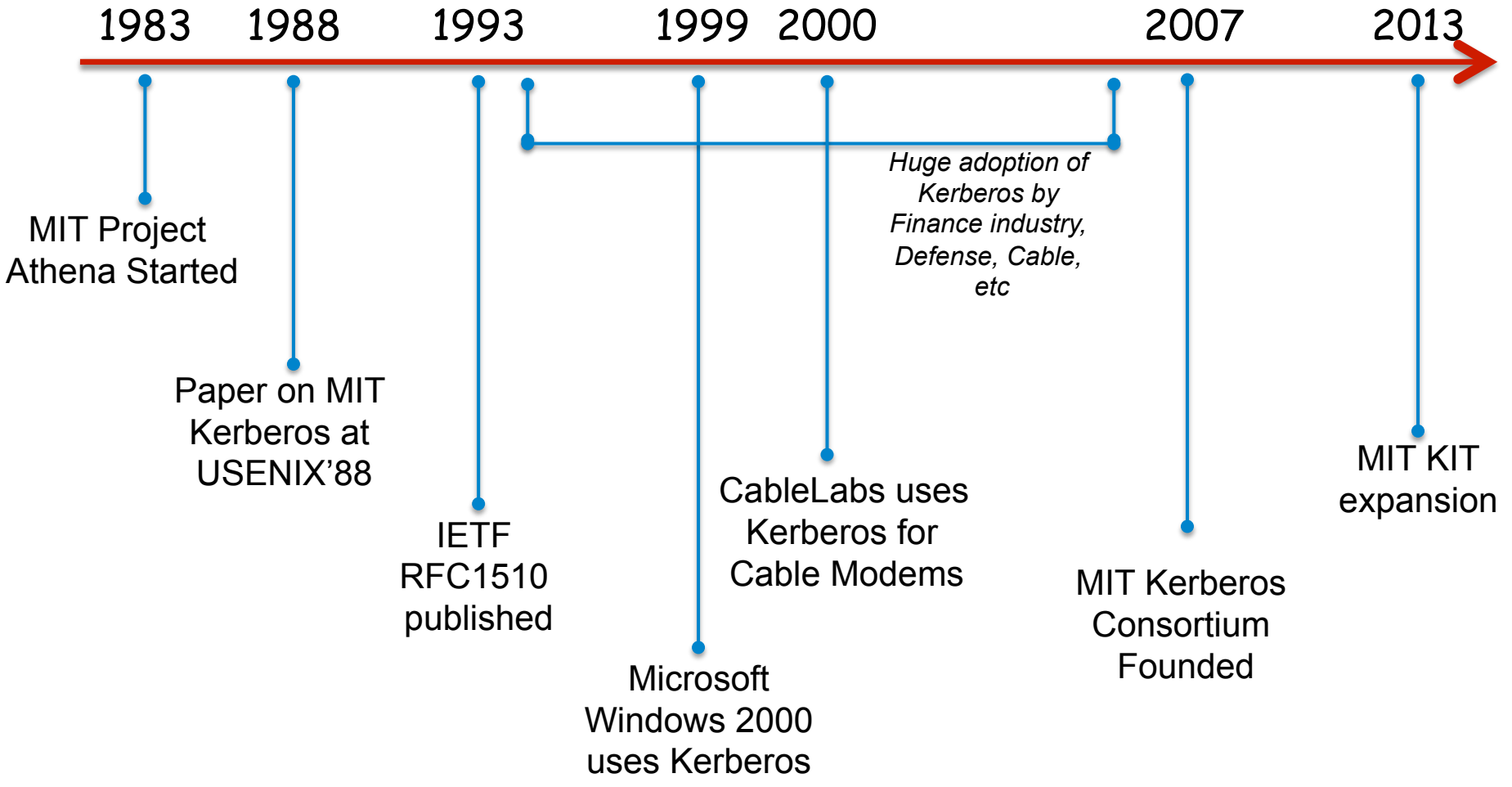
MIT KIT INTERNET TRUST

A Brief History of Kerberos

- Kerberos was developed as the Authentication engine for MIT's Project Athena in 1987:
  - Became IETF standard in 1993 (RFC1510) – now RFC4120
- MIT's release of Kerberos as open source in 1987 led to rapid adoption by numerous organizations
- Kerberos now ships standard with *all* major operating systems
  - Apple, Red Hat, Microsoft, Sun, Ubuntu
- Serves tens of millions of enterprise users:
  - Microsoft has been using Kerberos as the default authentication package since Windows 2000
  - Windows Logon used daily by millions of users.
  - Used in DOCSIS CableModems for device authentication.
  - Used for embedded systems security
- Kerberos has been *hugely* successful

MIT KIT INTERNET TRUST

MIT Kerberos: Timeline & Milestones



http://web.mit.edu/kerberos/papers.html

MIT KIT INTERNET TRUST

MIT Kerberos Consortium: Achievements

- Provide leadership to the world community in Kerberos authentication ✓ done
- Establish Kerberos as a ubiquitous authentication mechanism ✓ done
- Make Kerberos appropriate for new environments ✓ done
- Enable Kerberos across a plethora of endpoints ✓ done
- Help worldwide community of developers integrate Kerberos ✓ done

MIT KIT INTERNET TRUST

MIT Kerberos in Commercial Products

- Google
  - Enterprise Search Appliance (GSA)
- Cisco:
  - Cisco IOS - Rel. 11.2 +
  - NAC Appliance
  - ASA5000 & VPN3000 series.
- Intel:
  - VPro II Platforms (AMT)
- Red Hat:
  - Enterprise Linux & FreeIPA
- Sun/Oracle:
  - Solaris 8 to 10 and Solaris Nevada
- Yahoo
  - Hadoop infra
- Juniper:
  - Network Admission Control
- SAP R3
- NetApp:
  - Kerberized NFS
- F5 Networks:
  - BIG-IP ADC
- Other Open Source OS:
  - Ubuntu
  - Debian

MIT KIT INTERNET TRUST

Kerberos Projects: Completed & Underway

- MIT Kerberos code-base
  - Releases 1.7 to 1.13 (2007-2014)
  - Continuous (annual releases)
- Kerberos for Windows 4.0
  - For Windows-7 (64bit) onwards
  - Rev 4.1 due in Q3/2014
- Kerberos for Android (KFA):
  - Phase-1 completed (Proof of Concept)
  - Phase-2 (full Java-GSSAPI Bindings)
  - Completed in Dec 2012
- RxGK for AFS
  - Implement new GSSAPI based rxgk for RX (for AFS)
  - Project commenced in January 2013
  - Status: Seeking sponsors

MIT KIT INTERNET TRUST

MIT-KIT Mission

New Mission Statement (2013)

MIT KIT INTERNET TRUST

Mission Statement

“The Mission of the MIT-KIT is to develop the basic building blocks for the Internet's emerging personal data ecosystem in which people, organizations, and computers can manage access to their data more efficiently and equitably.”

kit.mit.edu

MIT KIT INTERNET TRUST

MIT-KIT: Purpose of Mission Expansion

- Provide leadership by addressing broader areas of Identity, Authorization and Privacy on the Internet
- Provide leadership, common ground and harmonization of current disparate solutions
- Deliver reference open-source code with high degree of interoperability
- Continue the MIT tradition of leadership & giving back to the world community
- Dedicate efforts to relevant Standards bodies

MIT KIT INTERNET TRUST

Deliverables

- Components (software)
  - New protocols and architectures
  - Specifications & standards
  - Modular software – open source
- Community (people)
  - International dev community
  - Bug reporting & patches
  - Interoperability testing
- Creativity (mind)
  - Ingenuity in solving difficult problems
  - Thought Leadership

MIT KIT INTERNET TRUST

Personal Data Ecosystem

The Emerging Ecosystem

MIT KIT INTERNET TRUST

Personal Data: The New Oil

- "*Personal data is the new oil of the Internet and the new currency of the digital world*"
  - Meglena Kuneva, European, Consumer Commissioner, March 2009
- Personal data "will emerge as a new asset class touching all aspects of society"
- Fundamental questions about privacy, property, global governance, human rights – essentially around who should benefit from the products and services built upon personal data – are major uncertainties shaping the opportunity.
- The rapid rate of technological change and commercialization in using personal data is undermining end user confidence and trust

Personal Data: Current State

- The current personal data ecosystem is fragmented and inefficient:
  - For many participants, the risks and liabilities exceed the economic returns.
  - Personal privacy concerns are inadequately addressed.
- Current technologies and laws fall short of providing the legal and technical infrastructure needed to support a well-functioning digital economy.
- Common needs for all users: Reliability, Predictability, Interoperability, Security, Ease of use, Cost-effectiveness, Risk and liability reduction, Transparency, Simplicity

MIT KIT INTERNET TRUST

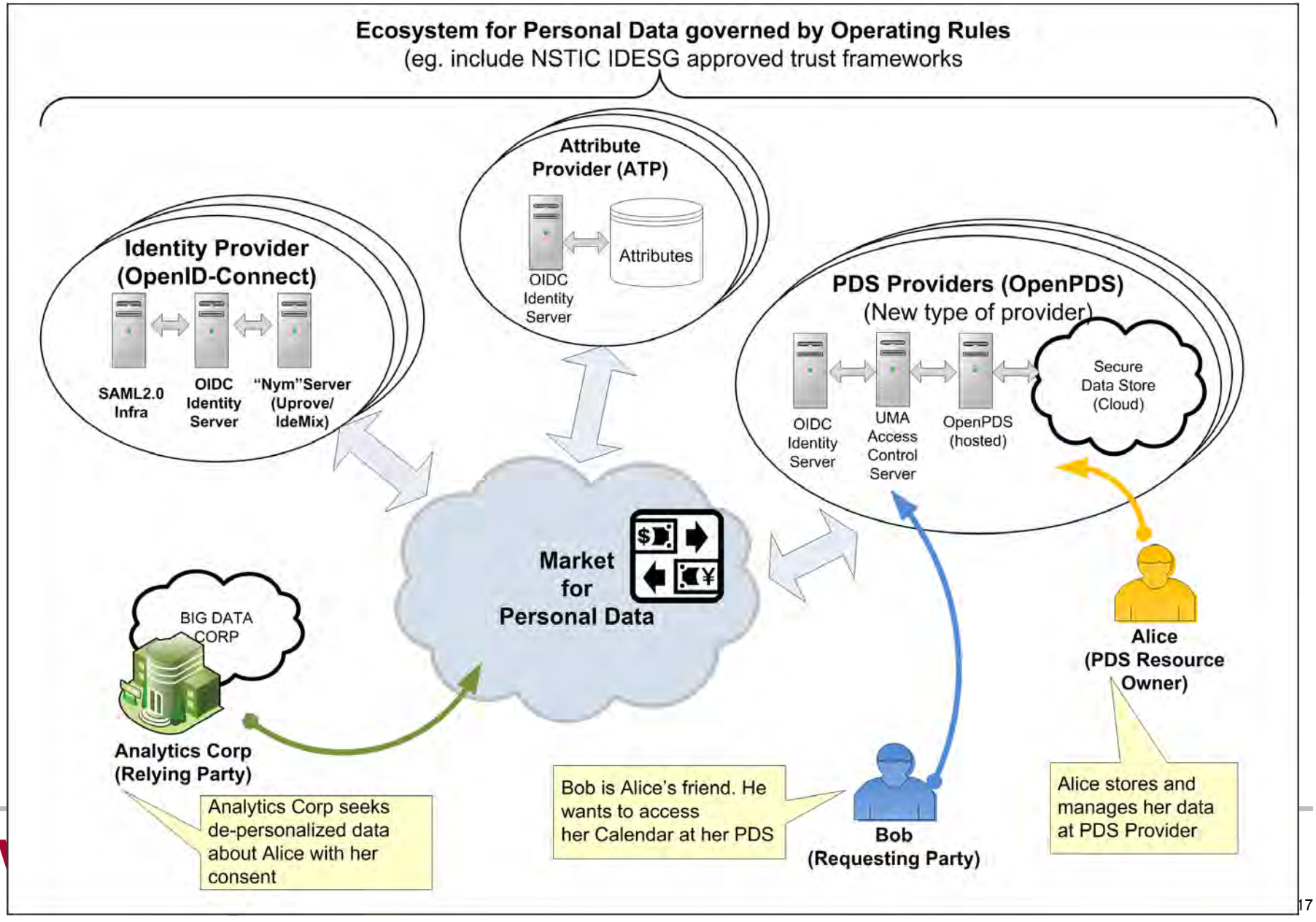
Personal Data: Way Forward

- *Alignment*: align key stakeholders (people, private firms and the public sector) in support of one another.
- *"Data as Money":* a person's data would be equivalent to their "money":
  - It would reside in an account where it would be controlled, managed, exchanged and accounted for just like personal banking services operate today
- *End-user centricity*: recognize that end-users are vital and independent stakeholders in the co-creation and value exchange of services and experiences.

Source: World Economic Forum, June 2010

MIT KIT INTERNET TRUST

Simplified Ecosystem View



Emerging Ecosystem Participants

- Identity Providers
  - Social Network players (eg. Google+, FB, Yahoo, etc)
  - NSTIC IDESG participants (numerous)
  - OIX and AXN members (numerous)
- Attribute Providers
  - Telcos, Banking & Finance
  - Gov orgs, State governments
  - Local Communities
- PDS Providers -- needed
  - Current offerings often called “personal clouds” - static data stores
- Cloud and Virtualization vendors & providers
  - Compute infrastructure to host PDS

References

- World Economic Forum: *Personal Data: The Emergence of a New Asset Class*, 2011 Report

  http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

- Alex (Sandy) Pentland, *Reality Mining of Mobile Communications: Toward a New Deal on Data*, The Global Information Technology Report 2008-2009, World Economic Forum.

  http://hd.media.mit.edu/wef_globalit.pdf

NSTIC IDESG

- Natl Strategy for Trusted Identities in Cyberspace
  - Identity Ecosystem Steering Group (IDESG)
- Vision of IDESG:

  "Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."
- Principles of IDESG: solutions must be
  - *Privacy-enhancing and voluntary*
  - *Secure and resilient*
  - *Interoperable*
  - *Cost-effective and easy to use*

MIT KIT INTERNET TRUST

https://www.idecosystem.org

MIT-KIT and NSTIC IDESG

- MIT is a member of NSTIC IDESG
  - Representative: Dazza Greenwood & Thomas Hardjono
- Trust Frameworks for Personal Data Ecosystem
  - Transparency of personal data (vs. “ownership” of data)
  - Baseline SLAs for Service Providers
  - Digital Contracts-Negotiation protocol
  - Standardized Trust Marks
- Some examples of marks:

MIT KIT INTERNET TRUST

https://www.idecosystem.org

MIT-KIT Personal Data Service

Personal “Big Data”: Philosophy

- Let people get equal access to their own data
  - Data generated by mobile devices, home appliances, cars, Tweets, posts, etc.
- Let people control & share their data
  - Help them understand & manage Consent
- Give people tools, applications & systems
  - Open-source, standards-based, easy to use
  - With strong privacy & security

MIT KIT INTERNET TRUST

Personal Data Service: Definition

A dynamic personal data service that has compute capability, portable, secure & easy to use.

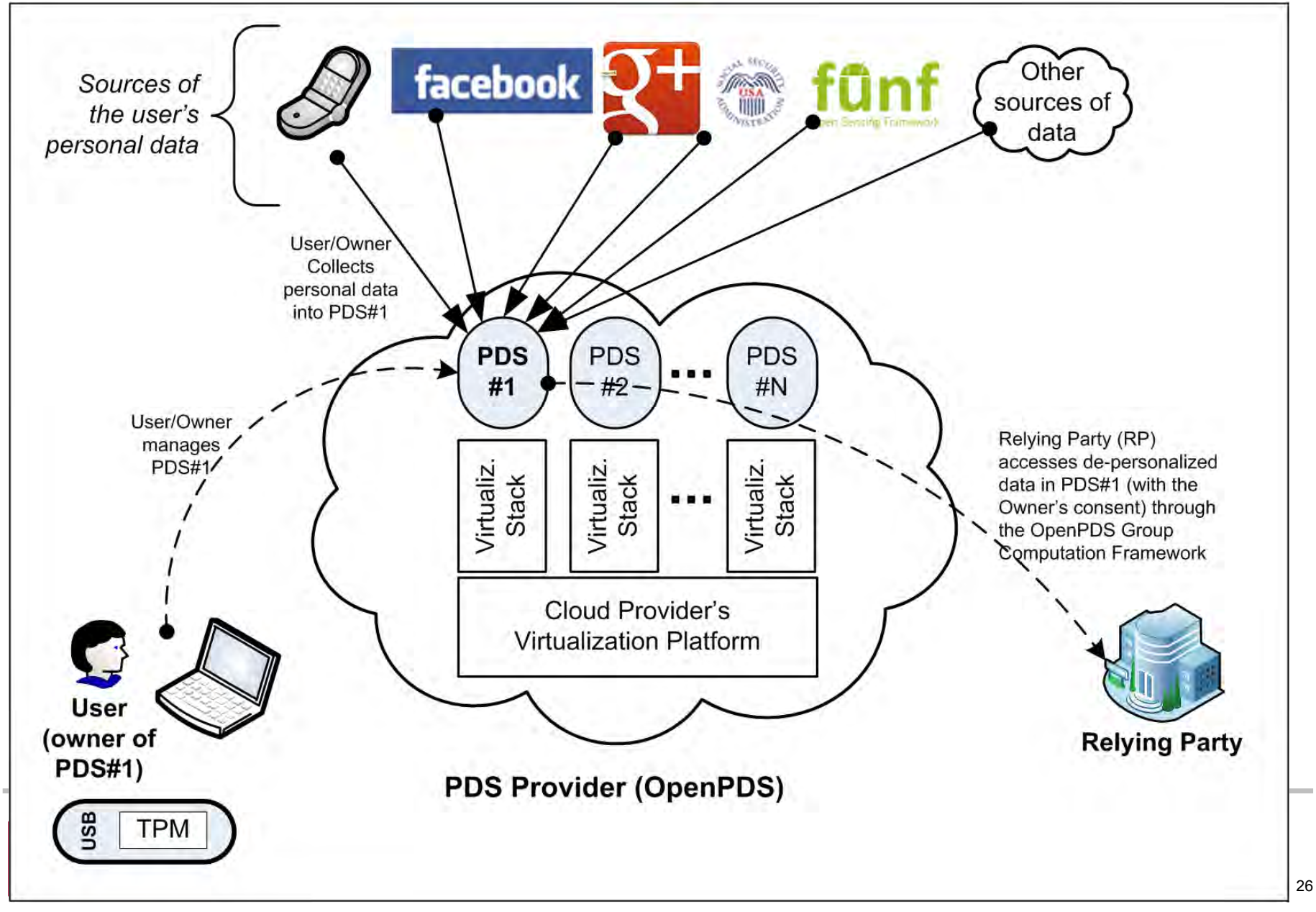
- Captures & retains data from user's devices
- Privacy-preserving, secure & owned legally
- Supports distributed & heterogeneous models
- Portable: moveable from one provider to another
- Exposes APIs for queries (privacy-preserving)

MIT KIT INTERNET TRUST

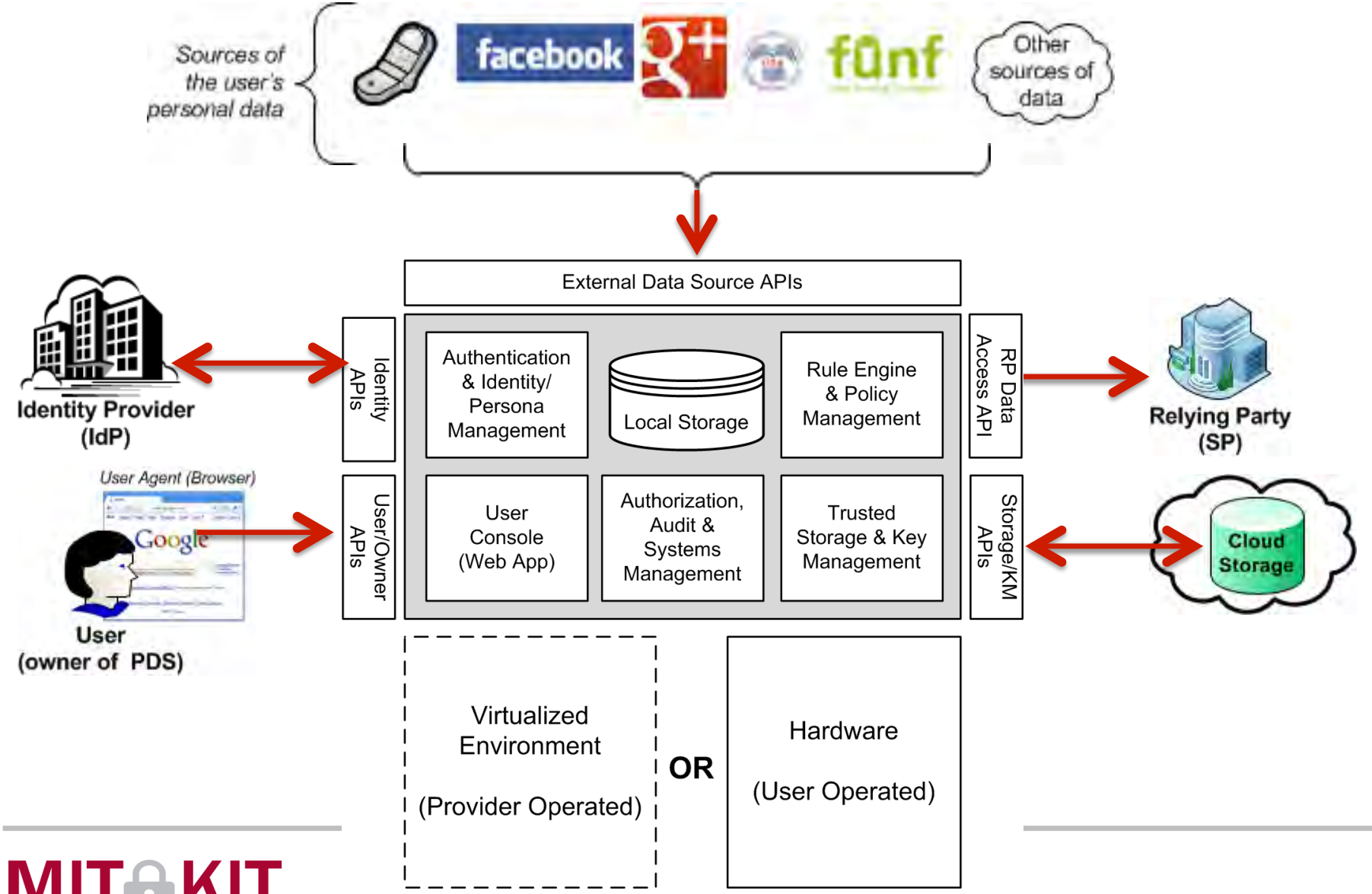
PDS: Services & Functions

- Authentication
- Authorization
- Identity Management & Federation
- Data privacy
  - cf. queries on user's encrypted data store
- Consent Management
  - Granting, tracking & revocations
- Policy management & Governance
- Many others…

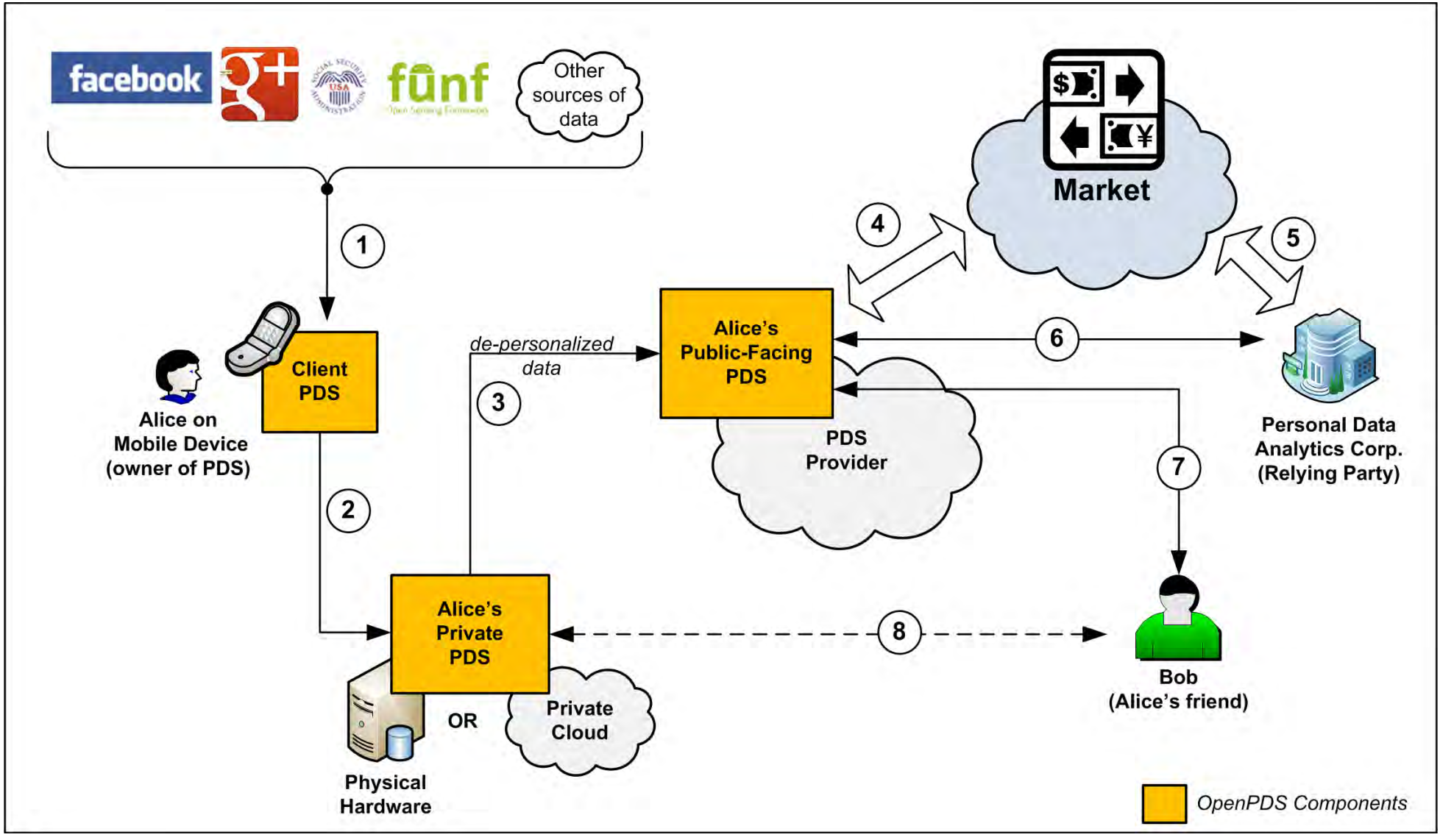
PDS in the Cloud



Technical Vision



PDS: Modular Components



Our Components Strategy

- PDS as umbrella provides guidance for selecting components/projects
- Different components for different deployments
- Bare-bones “Chassis & Engine Block” approach:
  - Vendors and users free to choose components
  - Build products around open-source components

We develop components

You build products/services

MIT-KIT Projects

- Kerberos (on-going)
- OpenID-Connect
- User Managed Access (UMA)

MIT KIT INTERNET TRUST

Criteria for Component Selection

- Supports goal/vision of building PDS
- Standardized Specifications
  - Component specification already RFC (or near RFC), or can be contributed to standardization bodies
- Standalone components useful
  - Components may be used/integrated for other use-cases
- Open Source
  - Under MIT License or compatible licenses
- Multiple implementations
  - Development community & Interoperability

MIT KIT INTERNET TRUST

Projects: Seeking Sponsors

- MITREid-Connect
- User Managed Access (UMA)
- Kerberos for the Cloud

Current Projects: MITREid OIDC

- MITREid-Connect for SSO in PDS:
  - OpenID-Connect (and OAuth2.0) implementation
    - Single-Sign-On (SSO) using OAuth2.0
  - Specifications from OpenID Foundation (OIF)
    - http://openid.net/developers/specs/
  - Source code donated from MITRE Corp.
  - Rev 1.0 released under Apache 2.0 & MIT-License
- OIDC used by OpenID Exchange (OIX) and AXN:
  - Google, Equifax, PayPal, VeriSign, Ping, NRI, etc
    - http://openidentityexchange.org
  - AXN: Attribute Exchange Network
    - http://openidentityexchange.org/projects/axn-pilots

MIT KIT INTERNET TRUST

kit.mit.edu/projects/mitreid-connect

Current Projects: MITREid OIDC

- Next rev features (planned):
  - Dynamic Registration
    - http://tools.ietf.org/wg/oauth/draft-ietf-oauth-dyn-reg/
    - In WG Last Call
  - Token Introspection
    - http://tools.ietf.org/id/draft-richer-oauth-introspection/
  - Token Chaining
- MITREid for Enterprise
  - Integration with SAML2.0 infrastructure
  - Kerberos ticket to token translation

MIT KIT INTERNET TRUST

kit.mit.edu/projects/mitreid-connect

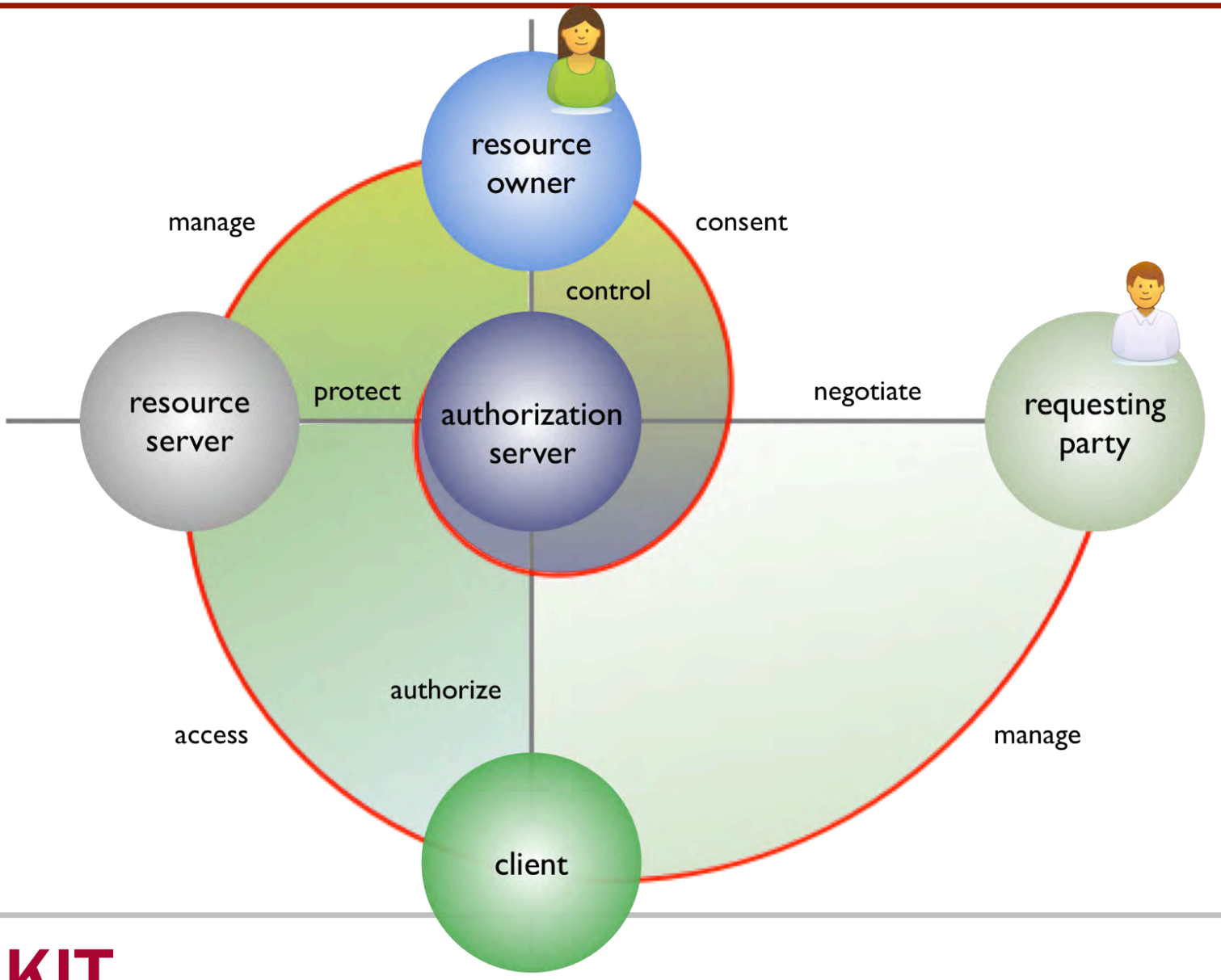
Seeking Sponsors: UMA Project

- UMA = User Managed Access
  - Extension or profiling of OpenID-Connect & OAuth2.0
- UMA is a Working Group in Kantara Initiative
  - http://kantarainitiative.org/confluence/display/uma
  - http://kantarainitiative.org/confluence/display/uma/UMA+1.0+Core+Protocol
- Specs contributed to IETF OAuth2.0 WG:
  - http://tools.ietf.org/id/draft-hardjono-oauth-umacore
  - http://tools.ietf.org/id/draft-hardjono-oauth-resource-reg
- Binding Obligations specification:
  - Identifies legal obligations of players within the protocol flow
  - http://docs.kantarainitiative.org/uma/draft-uma-trust.html
- Limited Implementations available (incomplete/proprietary)
  - Gluu, CloudIdentity (UK)

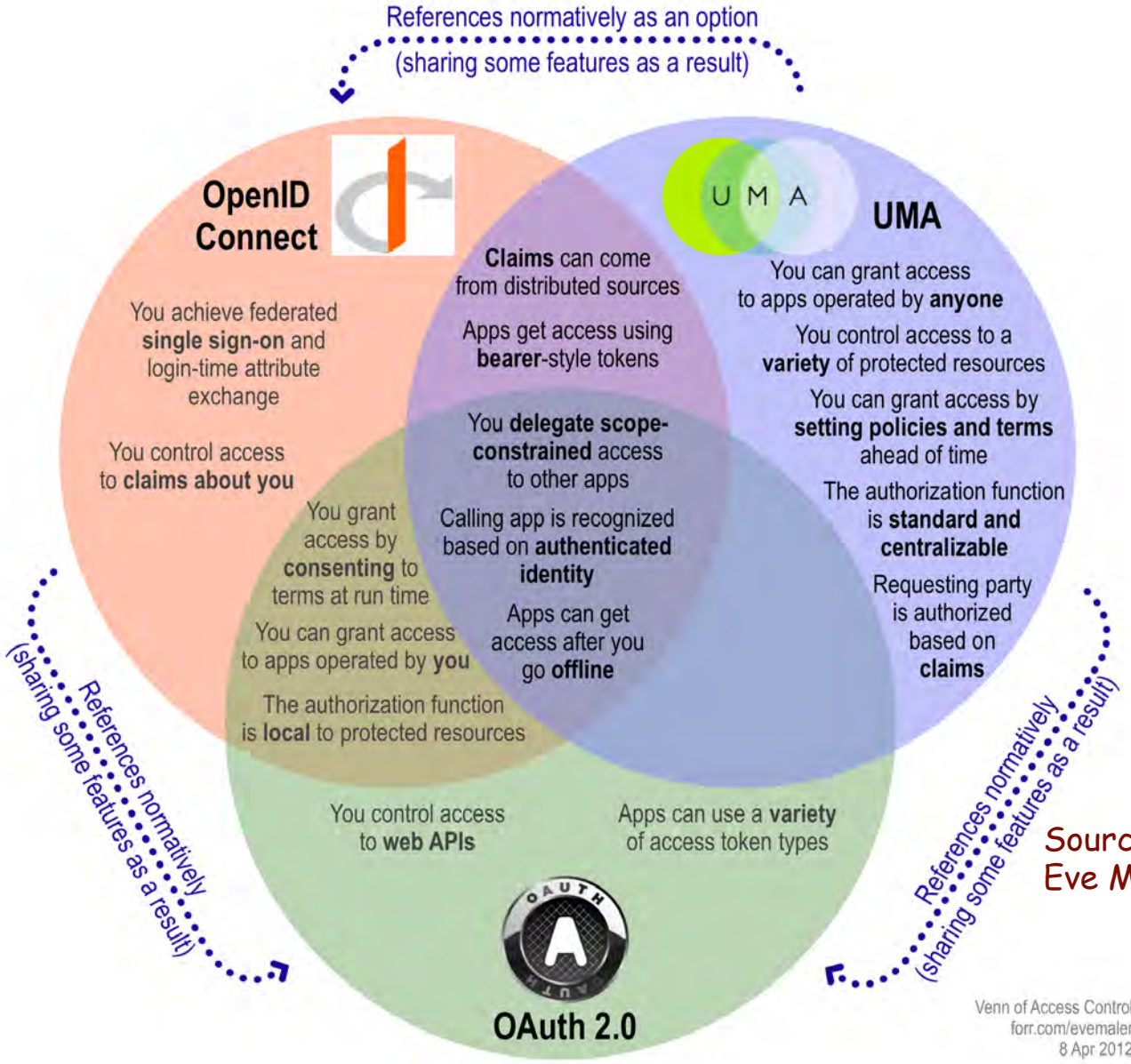
MIT KIT INTERNET TRUST

kit.mit.edu/projects/user-managed-access-uma

UMA: User-Centric Resource Sharing



UMA: Relationship with OAuth2.0 & OIDC



Source:
Eve Maler & UMA WG

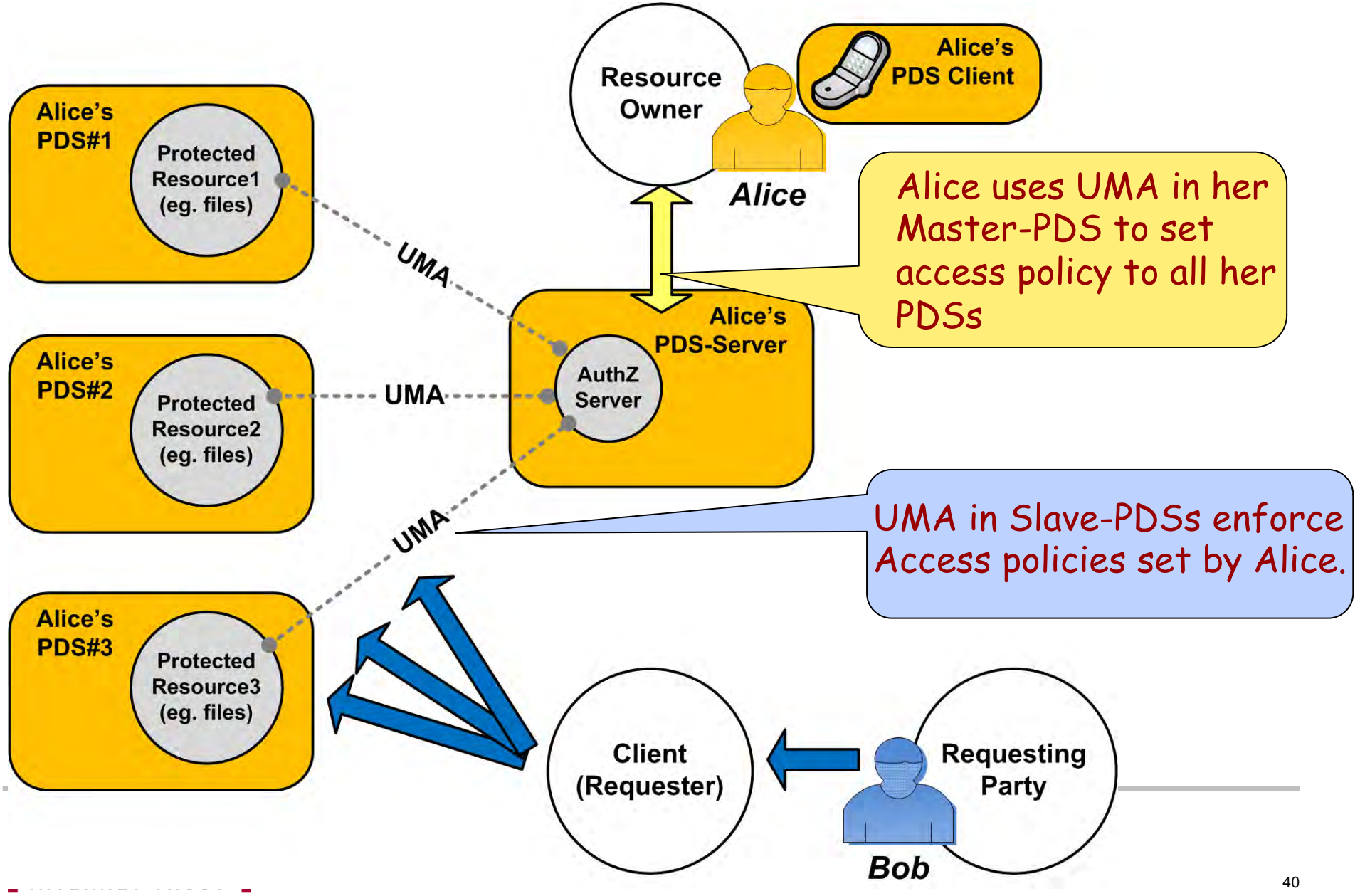
UMA for Access Control in MIT PDS

- UMA builds on OAuth2.0 and OpenID-Connect
  - Standardized OAuth2.0 token format (JSON/JWT)
  - Single-Sign-On (SSO) model follows OpenID-Connect
  - RESTful Web-APIs
- UMA supports distributed resource model
  - Reality today that User/Owner has files (e.g. photos, calendar, etc) distributed throughout the Internet
  - UMA's underlying PAP/PDP model fits MIT PDS architecture
- UMA supports linking of actions to obligations
  - Performing actions (as part of UMA protocol flow) results in both Owner and Requester/Requesting Party accepting mutually-agreed terms of service (or fragments of it)
  - Protocol flow vs. legal obligations flow

UMA for PDS: How

- UMA Authorization Server as PAP:
  - Policy Administration Point (PAP)
  - Single point where PDS-owner sets access policies
  - Across all PDS systems belonging to the Owner
  - Distributed access control model
    - Master-Slave model: Master-PDS with multiple Slave-PDS
    - Model used for distributed KDC in Kerberos
- UMA Authorization Server as PDP:
  - Policy Decision Point (PDP)
  - Access grant/deny decided by Authorization Server
  - Tokens granted and validated by Authorization Server

UMA for Access Control in PDS



Future Projects: An Open Invitation

- We welcome new members to the MIT-KIT:
  - Introduce your ideas & proposals
  - Engage MIT research community
  - Use the MIT-KIT as forum for discussion & development
  - Take leadership of projects
- Potential new projects:
  - Anonymous credential system
  - Anonymous verifiable attributes
  - Homomorphic & Functional encryption of data in PDS

MIT KIT INTERNET TRUST

Current MIT-KIT Members

Community Members

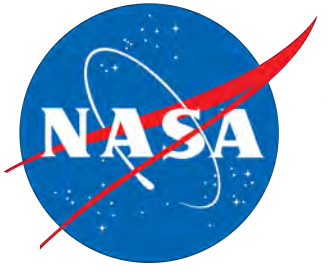
- CMU
- Centrify Corporation
- Columbia University
- Cornell University
- US DOD
- **Fidelity** *
- Iowa State University
- **MIT** *
- Michigan State niv
- **MITRE** *
- **Microsoft** *
- **Morgan Stanley***
- NASA
- **NetApp** *
- **Nippon Telephone and Telegraph (NTT)***
- **Oracle/Sun** *
- Pennsylvania State Univ.
- **Red Hat** *
- TeamF1, Inc.
- The University of Michigan
- The U. of Pennsylvania
- Stanford U.
- (Google)

MIT KIT INTERNET TRUST

* = Advisory Board Member

Community Members

Cornell University



Jet Propulsion Laboratory
California Institute of Technology

UNIVERSITY of ALASKA

MIT-KC Board Members

Company	Name	Title/Role
Microsoft	Slava Kavsan	Chief Architect, Windows Security & Azure
Oracle	Eric Kozlowski	Snr. Manager, Solaris Security
NTT	Satoru Kanno (Dr. Masayuki Kanda)	VP, Security and Crypto, NTT Software
NetApp	Satyajit Deshmukh	Snr. Manager
Fidelity	Rajan Kulkarni	Chief Architect, Fidelity Center for Applied Technology
Red Hat	Dmitri Pal	Snr Manager, Enterprise Linux Security
MIT	Mark Silis	Director of Network Infrastructure
MITRE Corp	Dr. Joshua Guttman	Lead Scientist
Morgan Stanley	Ish Ahluwalia	Director of Infra Security

Academic Advisory Board

Organization	Name	Title/Role
MIT Media Lab	Prof. Sandy Pentland	Toshiba Professor of Media & Society
Brown University	Prof. Anna Lysyanskaya	Professor of Computer Science
RSA Inc	Dr. Ari Juels	Chief Scientist
MITRE Corp	Dr. Joshua Guttman	Lead Scientist
MIT CSAIL	Dr. Nickolai Zeldovich	Assoc. Professor
NTT Japan	Prof. Tatsuaki Okamoto	Founder & Director of Okamoto Laboratories in NTT

***Prof. Ron Rivest, CSAIL, MIT**

MIT KIT INTERNET TRUST

Membership & Benefits

Board Membership Benefits

- Easy access to experts
  - Core team, consultants and developers worldwide
- Special Projects
  - Fast-track special requests
  - Integrate into multi-year code releases
- Features Request
  - Priority for new features for next release
- Guidance in Deployment, integration & upgrades
  - Technical review of plans
  - F2F meetings
- Influence on project evolution
- Full view into development roadmap

MIT KIT INTERNET TRUST

Fee Structure: Summary

- Advisory Board Member:
  - $50K annually for 3 years
  - Co-designed, sponsor-focused special project
  - Voting seat on Advisory Board
  - Full view into roadmap
- Patron Sponsor:
  - $25K annually for 3 years
  - Complimentary participation in workshops and interoperability testing events.

MIT KIT INTERNET TRUST

Contact Information

The MIT Kerberos & Internet Trust (KIT) Consortium
77 Massachusetts Avenue
W92-152
Cambridge, MA 02139 USA

kit.mit.edu

Thomas Hardjono, PhD.
Technical Lead & Executive Director

Email: hardjono@mit.edu
Mobile: +1 781 729 9559
Twitter: @FindThomas

Web: kit.mit.edu