MIT Kerberos & Internet Trust Consortium

Mission & Vision

May 2014
Contents

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

Kerberos: 1987 - today
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 Kerberos: Timeline & Milestones

1983
- MIT Project Athena Started

1988
- Paper on MIT Kerberos at USENIX’88

1993
- IETF RFC1510 published

1999
- Microsoft Windows 2000 uses Kerberos

2000
- CableLabs uses Kerberos for Cable Modems

2007
- MIT Kerberos Consortium Founded

2013
- MIT KIT expansion

Huge adoption of Kerberos by Finance industry, Defense, Cable, etc

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

© 2014 The MIT Kerberos & Internet Trust Consortium. All Rights Reserved. – kit.mit.edu
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 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
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 Mission

New Mission Statement (2013)
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.”
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
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
Personal Data Ecosystem

The Emerging Ecosystem
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
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
Simplified Ecosystem View

Ecosystem for Personal Data governed by Operating Rules
(eg. include NSTIC IDESG approved trust frameworks)

Identity Provider (OpenID-Connect)
- SAML2.0 Infra
- OIDC Identity Server
- "Nym"Server (Uprovel IdeMix)

Attribute Provider (ATP)
- OIDC Identity Server
- Attributes

PDS Providers (OpenPDS)
- New type of provider
- Secure Data Store (Cloud)
- OIDC Identity Server
- UMA Access Control Server
- OpenPDS (hosted)

Market for Personal Data

Analytics Corp (Relying Party)

BIG DATA CORP

Bob is Alice’s friend. He wants to access her Calendar at her PDS

Bob (Requesting Party)

Alice stores and manages her data at PDS Provider

Alice (PDS Resource Owner)

Analytics Corp seeks de-personalized data about Alice with her consent
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://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

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:

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
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)
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…
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)
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
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

kit.mit.edu/projects/mitreid-connect
Current Projects: MITREid OIDC

- Next rev features (planned):
  - Dynamic Registration
    - In WG Last Call
  - Token Introspection
  - Token Chaining
- MITREid for Enterprise
  - Integration with SAML2.0 infrastructure
  - Kerberos ticket to token translation
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

• 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)

kit.mit.edu/projects/user-managed-access-uma
UMA: User-Centric Resource Sharing

- Resource owner
- Authorization server
- Client
- Requesting party

Actions:
- Manage
- Consent
- Control
- Negotiate
- Protect
- Authorize
- Access
- Manage
UMA: Relationship with OAuth2.0 & OIDC

**OpenID Connect**
- You achieve federated single sign-on and login-time attribute exchange
- You control access to claims about you

**UMA**
- You can grant access to apps operated by anyone
- You control access to a variety of protected resources
- You can grant access by setting policies and terms ahead of time
- The authorization function is standard and centralizable
- Requesting party is authorized based on claims

**OAuth 2.0**
- You control access to web APIs

**Claims**
- Claims can come from distributed sources
- Apps get access using bearer-style tokens
- You delegate scope-constrained access to other apps
- Calling app is recognized based on authenticated identity
- Apps can get access after you go offline

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

Alice uses UMA in her Master-PDS to set access policy to all her PDSs. UMA in Slave-PDSs enforce Access policies set by Alice.
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
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)

* = Advisory Board Member
Community Members
# MIT-KC Board Members

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

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

*Prof. Ron Rivest, CSAIL, MIT*
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
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.
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