Kerberos Revisited

Quantum-Safe Authentication

M. Campagna (mcampagna@gmail.com), T. Hardjono (MIT), L. Pintsov (Pitney Bowes), B. Romansky (Pitney Bowes) and T. Yu (MIT)

ETSI Quantum-Safe-Crypto Workshop

September 26, 2013

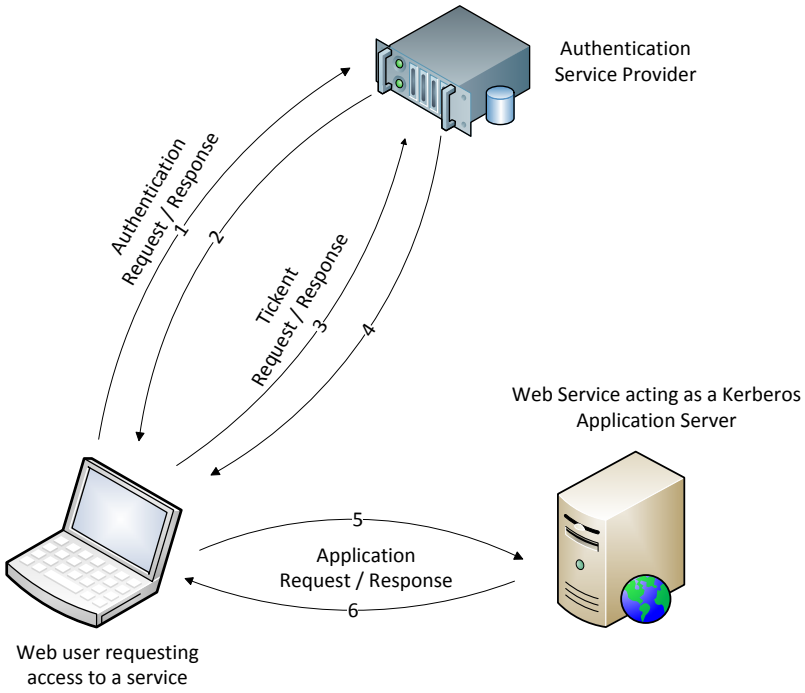
Participants

- The Mission of the MIT-Kerberos and Internet Trust Consortium (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.
- Pitney Bowes is a provider of cryptographically secure payment and data management systems to worldwide postal and logistics community. Pitney Bowes developed, built and operates a broad information security infrastructure supporting over 2M users worldwide.

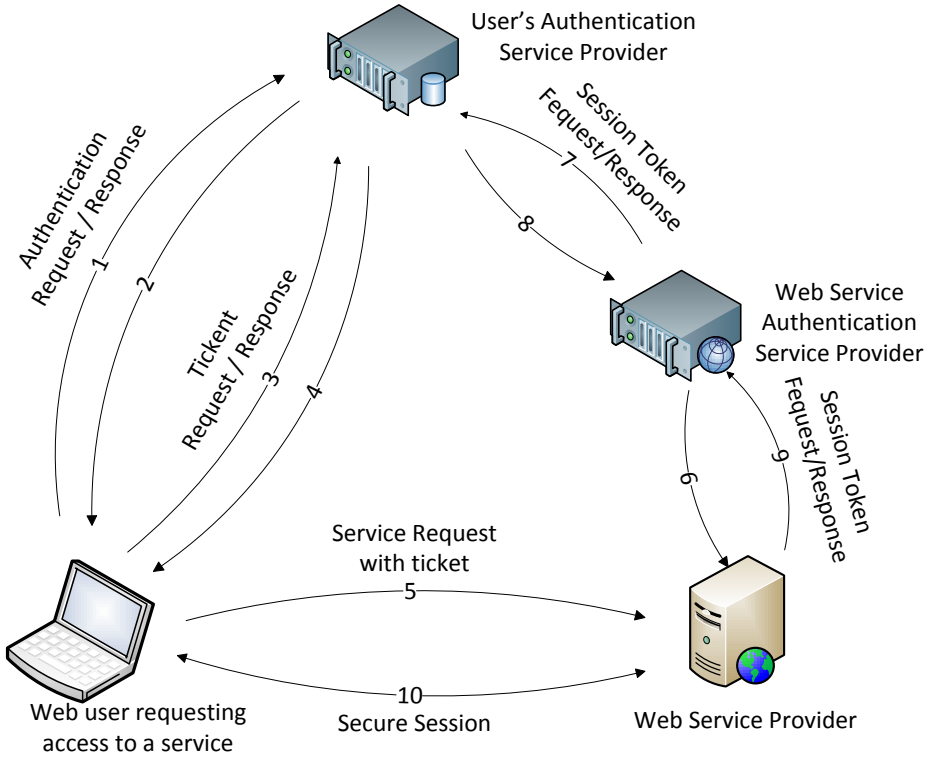
Motivation

- Quantum computing field is 20 years old
  - Significant theoretical progress (Shor's results, error-correction "threshold" theorem)
  - Meaningful experimental progress
    - 5 qubit to 128 or even 439 qubit (D-Wave computer, although it does not make use of entanglement)
- It is not unreasonable to assume that working quantum computer may become a reality in the foreseeable future
- Classic public key algorithms that are based on hardness of factorization and discrete logarithm problems may become vulnerable
- A "good" symmetric key based-system may prove to be very beneficial in many applications
- MIT-KIT, M. Campagna and Pitney Bowes have common research interest in investigation, development and test of a broadly scalable quantum-safe solutions for Identity and Access Management

Kerberos Models



Single-Provider Model



Cross-Realm Federated Model

Requirements

- Quantum Safe
- Support Authentication and Federated Identity System
- Deployable on an “internet scale” – every user, multiple devices, multiple providers, …
  - Establish secure communications to remote servers/networks (must enable traditional security services: authenticity, integrity and secrecy and non-repudiation of message content)
- Designed for Usability
  - Accessibility, convenience, intuitiveness
  - Optimum balance between security and usability

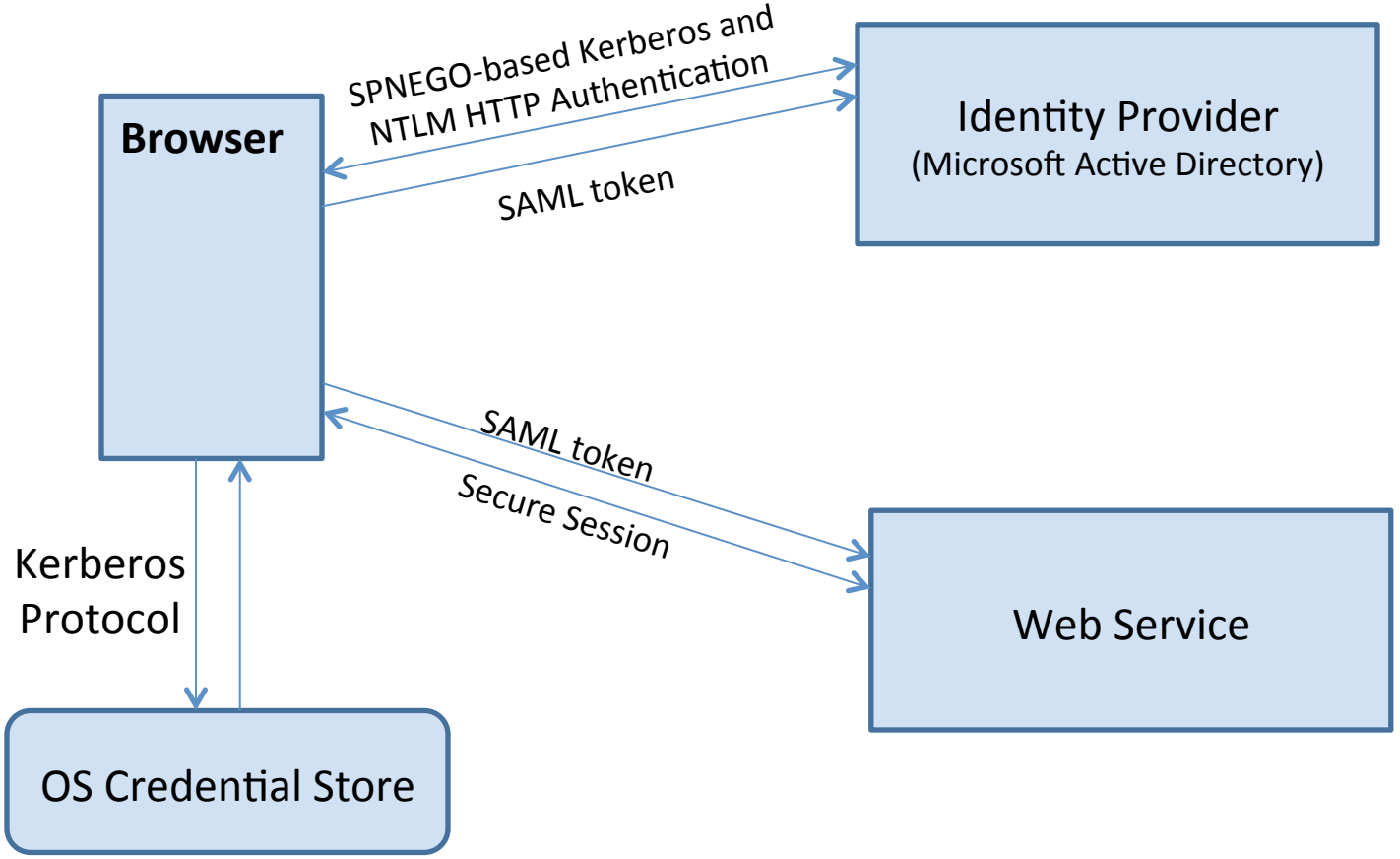
Kerberos Challenges

- Development
  - Need good APIs and tools to enable developers to build on the existing Kerberos system
- Federation
  - Service providers should be enabled to integrate technology into their offering to establish a chain of trust
- Enrollment
  - Must be efficient, secure, and convenient for the end users
- Administration
  - Must be efficient, secure, and operable at scale

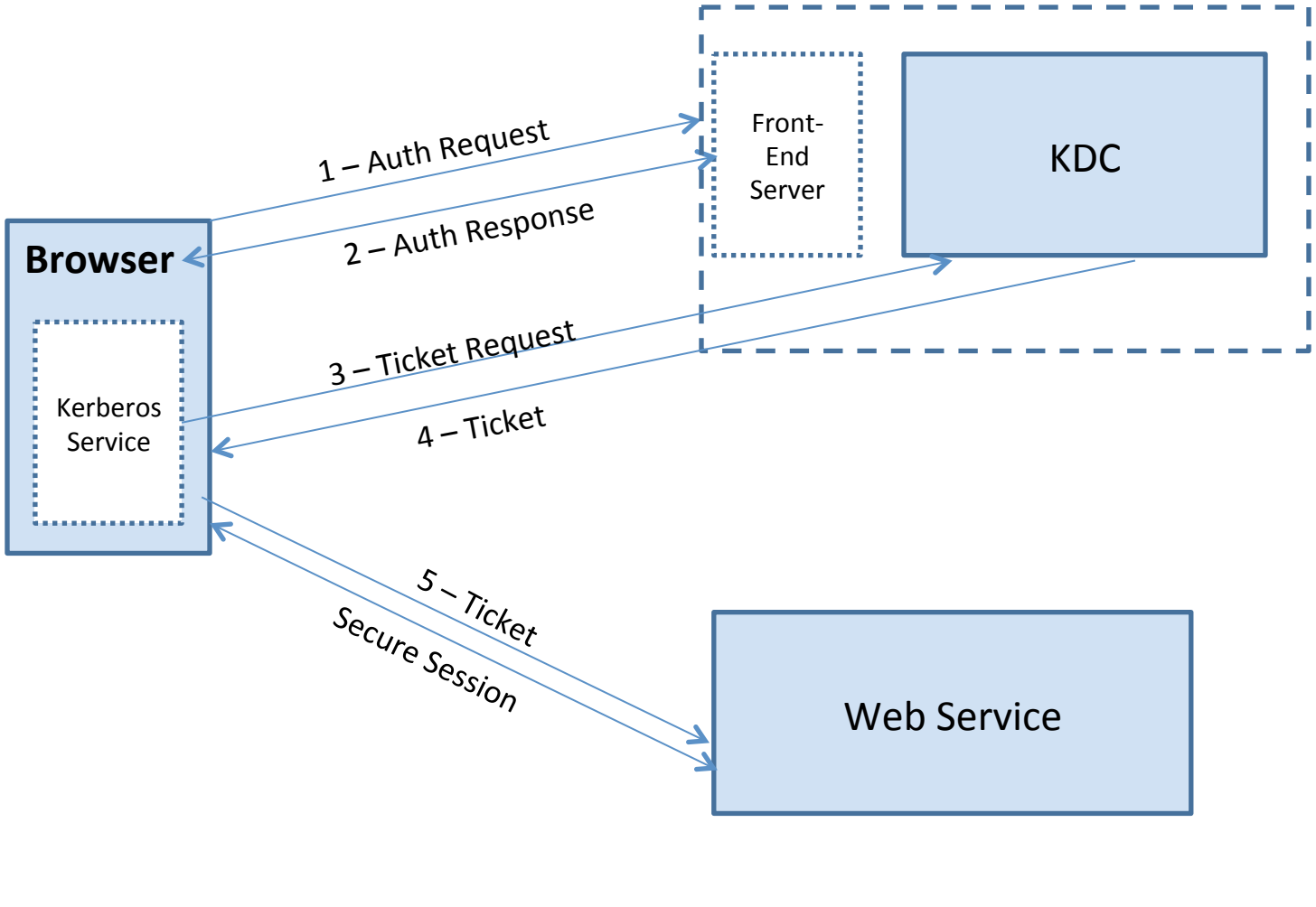
Development and Implementation

- Need a RESTful services API that give access to the Kerberos protocol
  - Enable access to Kerberos without going through GSSAPI
- Software, tools, integration, and deployment
  - Example: model after OpenSSL or other popular web implementations
- Develop tools with application development and specific use cases in mind

Current Web Services Access Protocol



Kerberos-Based Service Access Protocol



Enrollment

- Provision a long-term symmetric key that is not password derived (for each user, and possibly each device)
  - Strongly random and securely distributed and installed
- Options
  - Use existing relationship between end users and commercial establishments (employers, banks, etc.)
  - Device based – pre-installed keys
    - Keys to be issued by a device manufacturer or a carrier at time that device is manufactured or delivered. Root of trust for each device starts with the manufacturer or carrier
    - Financial arrangement with a primary user establishes the identity of the accountable user – users may delegate their rights on their device to others (i.e. the accountable user could become the “RA”)
  - Retail channels to acquire credentials
    - Postal Infrastructure
    - Retail Kiosks
  - Social – PGP-like model (peer to peer chain of trust)
  - Quantum Key Distribution
    - ComDev/IQC proposal for quantum key distribution via microsatellites

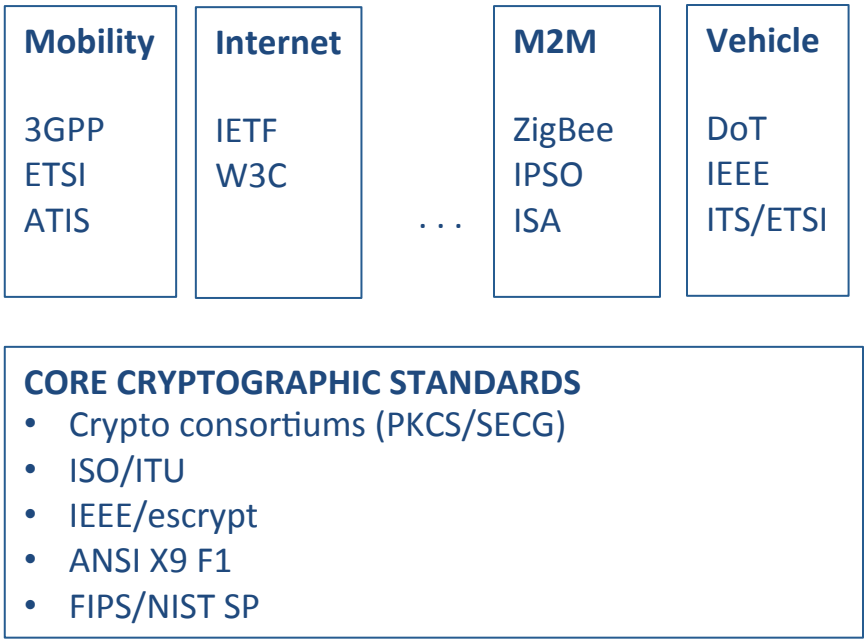
Federation

- Need a “critical mass” of KDC and AS operators
  - Every user must have a relationship with one or more provider and they must trust the provider to manage their identity
  - They need to do cross-realm authentication
- “Standard” contracts to establish “legal trust”
  - NSTIC process may provide templates
- Need for an accreditation and audit protocol and authority
- Establishing federation today is harder than it ought to be

Administration

- Physical (hardware) security can improve trust in providers
- Time synchronization issues
- Dealing with compromise or loss of user credentials
- Compromise of a KDC
  - Need to continue operations and recover
  - Consumers will likely require multiple authentication services providers

Stack model view of cryptographic standards



Cryptographic standards have wide applicability across many industry spaces

Most influential specifications have the widest adoption–e.g. FIPS/NIST SP

Vertical markets generally adopt from specific core standards

Adoption requires that specs are freely available and timely

Role of Standards

- For any wide-spread quantum-safe solution:
  - Cryptographic primitives need to be widely accepted by international and national standards bodies, like FIPS, ANSI and ISO;
  - Higher level protocols and use cases need to be specified in IEEE, IETF and other application-specific standards bodies.
- Current advantages of Kerberos:
  - Kerberos is already accepted as a trusted and tested protocol which is agile to the underlying cryptographic primitives;
  - Already integrated in every major platform;
  - Uses widely adopted and tested cryptographic primitives, and specified in higher level protocols
- Standardization Process
  - Primitives – ANSI / NIST
  - Algorithms – IETF / IEEE

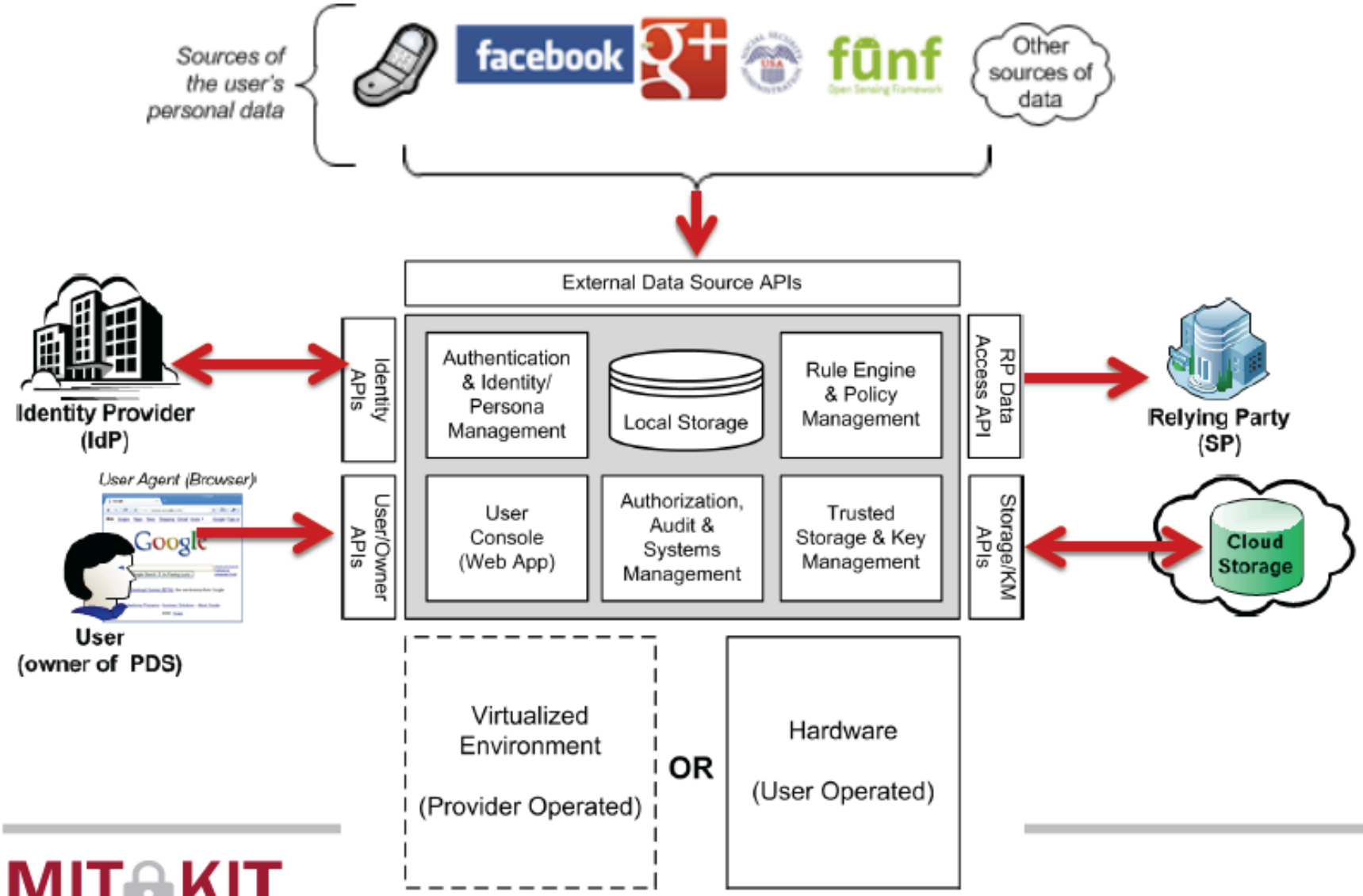
Infrastructure requirements

- Virtual environments make it difficult to ensure trust
- Hardware Security Module or “Virtual Trusted Platform Module ” technology may be needed
- Concept – segment the KDC architecture and create a secure co-processor that provides crypto-acceleration and secure key storage
- Need a spectrum of solutions that make different trade-offs on scale and trust
  - Need to define metrics to describe the security levels and make users aware of the meaning of the different levels

Digital Signatures and Non-Repudiation

- Digital signatures require a third party notary service provider
  - Verification must be done online
- Existing symmetric-key digital signatures have potential, but are not efficient
  - Example: Lamport-Merkle scheme

OpenPDS: Technical Vision



MIT KIT INTERNET TRUST

Conclusion

- There is nothing inherent in the Kerberos protocol that prohibits use in a wide-scale, federated deployment
- Standards are critical for wide scale implementation
  - Integration of Kerberos with web services and internet applications
  - Federation, certification, and auditing standards for service providers
  - Template agreements to initiate trust relationships
- Maintenance of both open source (with a permissive license) and commercial implementations could support expedited integration and adoption
- We identified and sketched major challenges to adoption of the Kerberos-based system into deployable Internet scale authentication system