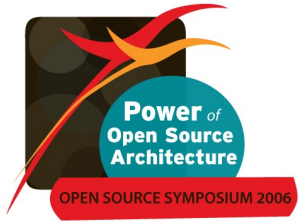
Security and ID Management
Keeping your business safe

Satish Chetty
Technical Support Account Manager
Red Hat Inc.



Identity and Security Management

- Identity and Security Management is the secure control of user information and access rights across multiple systems and business contexts.

  Providing:

  - **Improved User Productivity**

    Timely, Personalized Access to applications, systems, and resources

  - **IT Management Efficiency**

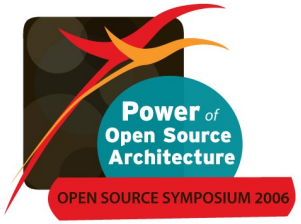
    Simplified management tasks and reduced requests

  - **Application Development**

    Reusable identity and security components

  - **Auditing and Compliance**

    Ensuring business meets the latest regulations and requirements.

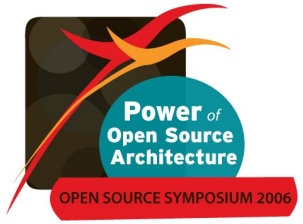


Identity and Security Management

- Simplify management of increasingly complex environments
- Provide the benefits of Open Source to all components of an enterprise deployment
  - Systems, Identity, Security
- Provide a path for integrated identity and security control
  - Systems, Application and User Management within a common console
  - Single sign on
  - Secure messaging
  - Directory enabled applications
  - Stateless Linux

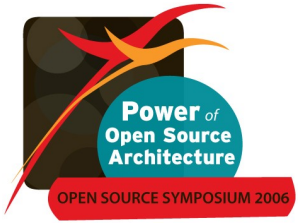
Control of Access

- Identification: The entity makes claim to a particular identity
- Authentication: The entities prove that they are who they say they are
- Authorization: The entity is granted certain access rights based on the Authenticated Identity



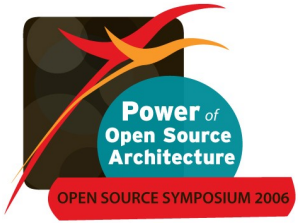
Multi-factor Authentication

- Something you know: PIN, Password, Picture
- Something you have: Token, card, Certificate
- Something you are: Biometrics, fingerprints, Iris Scan, Hand Geometry, Voice Print or Facial Image



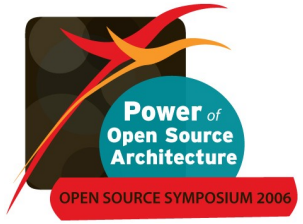
Reasons?

- Regulatory Requirements
- Security Benefits
- Economic Benefits
- Usability Benefits



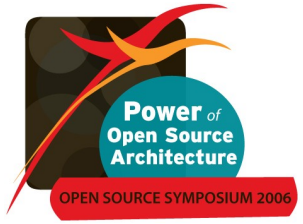
Regulatory

- HSPD 12
- FIPS 201
- Sarbanes Oxley



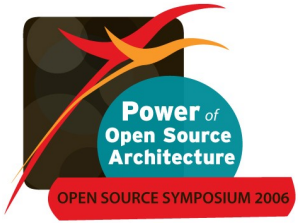
Security Benefits

- Digital Identity
- Authenticity and Integrity
- Strong Authentication
- Data Encryption
- Non Repudiation



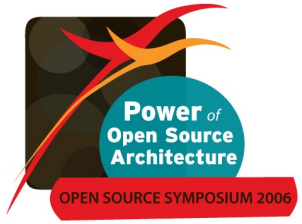
Economic Benefits

- Reduced Help desk calls
- Consolidate Multiple Functions to one token
- Consolidate physical and local access



Usability Benefits

- End User Convenience



Smart Cards

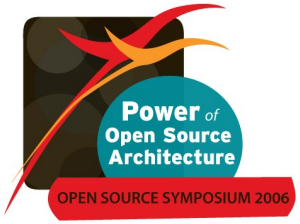
- Pros
  - Can store photo, smart chip and antenna in one token
  - PKI enables encryption and assures content is secure
- Cons
  - Card readers are not ubiquitous
  - User acceptance issues

USB Tokens

- Pros
    - Benefits of a smart card
    - USB ports readily available
- Cons
    - Cannot be used for physical identification only logical access

OTP Tokens

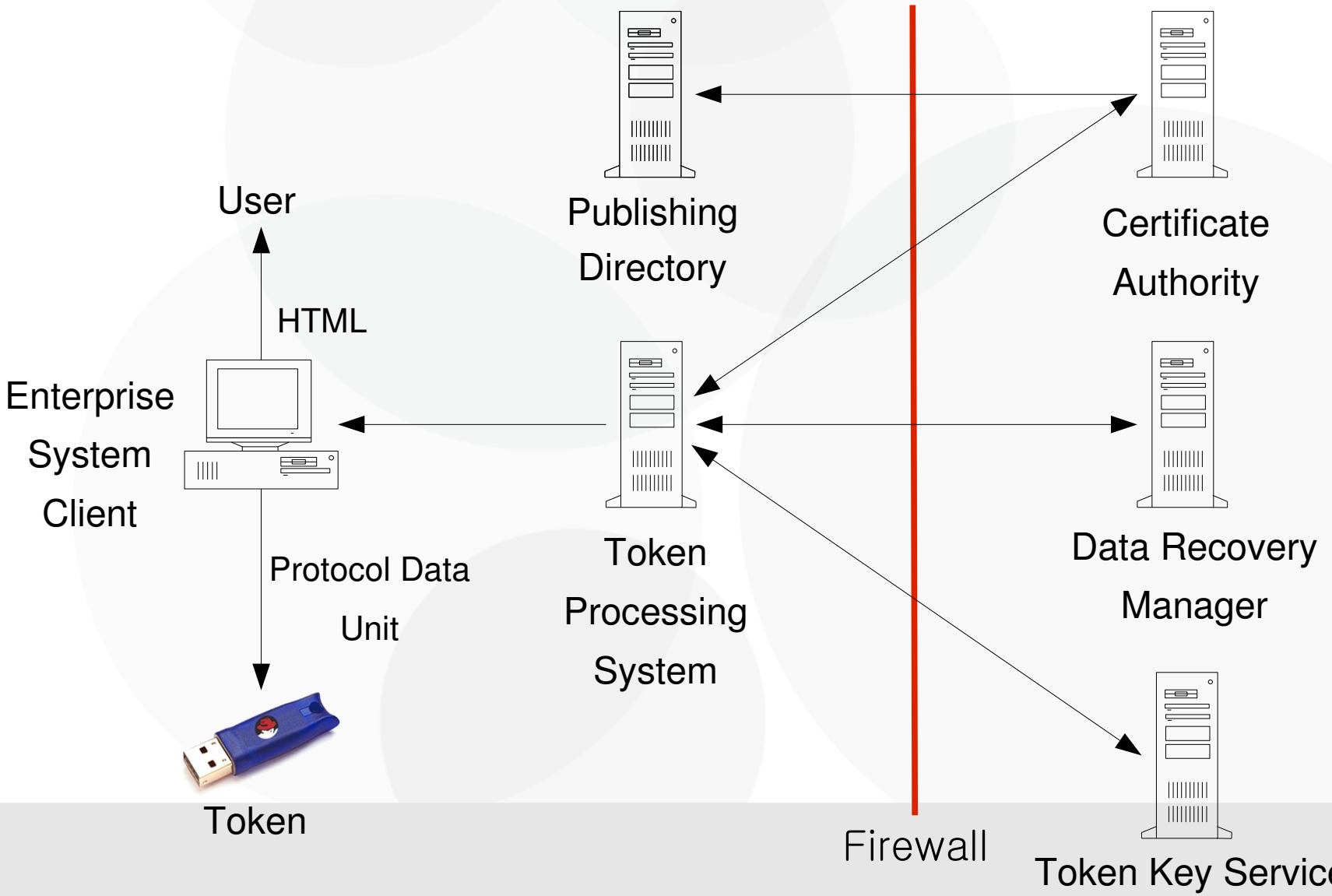
- Pros
    - No hardware reader required
    - No local client software required
- Cons
    - Logical access only no physical identification
    - Can have a clumsy UI
    - Cannot be used for PKI operations
    - Prone to phishing

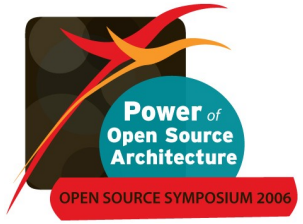


Software Tokens

- Pros
  - No separate hardware token or reader required
- Cons
  - Vulnerable to automated attacks
  - Does not provide non-repudiation

Token Management System





Revocation

- Certificate Authority periodically issues Certificate Revocation List (CRL)
- Revocation Reasons:
- Key compromise or loss
- Change of affiliation
- Relying Parties are supposed to check the CRL when verifying a certificate
- Certificates expire after a period of time
- They can then be removed from the CRL


Power of
Open Source
Architecture
OPEN SOURCE SYMPOSIUM 2006

Questions