

# eGovernment

---

**Large Scale Consumer  
eAuthentication**

**Khaja E. Ahmed  
CTO – MS Passport**

# Agenda

- **Discuss an approach to consumer authentication services**
- **Passport**
  - **What it does**
    - **Different types and levels of auth**
    - **Allow anonymous / pseudonymous IDs**
    - **Allows multiple IDs**
    - **Allow strong authenticated IDs (3.0)**
  - **What it does not do**
    - **Identity verification**
    - **ID management**
- **Microsoft – Advise, Standards, Products, Services, Standards, Development tools**

# Identify, Authenticate, Authorize

- **Identification** – The determination of the identity (or credential) of a principal
- **Authentication\*** – The verification of an identity claim
- **Authorization** – The decision to grant a privilege or permission

# Consumer eAuthentication

## ...required coordinated-parts

- **Economic Models to make this viable**
- **Governance / Operating Rules**
  - **Policies / procedures / compliance with Law**
  - **Audit requirements**
  - **Arbitration / dispute resolution**
- **Technology**
  - **Interoperable standards / protocols**
  - **Products**
    - **Widely available**
    - **Well supported**
- **Operations**
  - **Services**
  - **Physical and virtual locations**

**Microsoft®**

# **Economic Model**

## **...economically viable**

- **Economic / Business Model for all the service providers**
  - **Registration Authorities**
  - **Identity Issuance Authorities**
  - **Identity Verification Service**
  - **Service consumed**

# **Governance**

## **...Legally valid**

- **Policies / Procedures / agreements**
  - **Uniform across the ‘community of trust’**
- **Compliance with laws of applicable Jurisdiction**
  - **Cross Jurisdiction enforceability**
- **Legal Recourse**
- **Consumer protection**
- **Privacy and security of PII**
- **Audit and Verification process**
- **Arbitration / Dispute resolution**

# Technology

## ...technologically feasible

- **Standards**
  - **Allows large population of Identity Issuers and Service providers to work together**
  - **Allows large number of product developers to build products and applications that use such services**
- **Products / Tools**
  - **Ubiquitous availability of interoperable products is a requirement for consumer facing services**
  - **Products need to be widely supported and accessible**

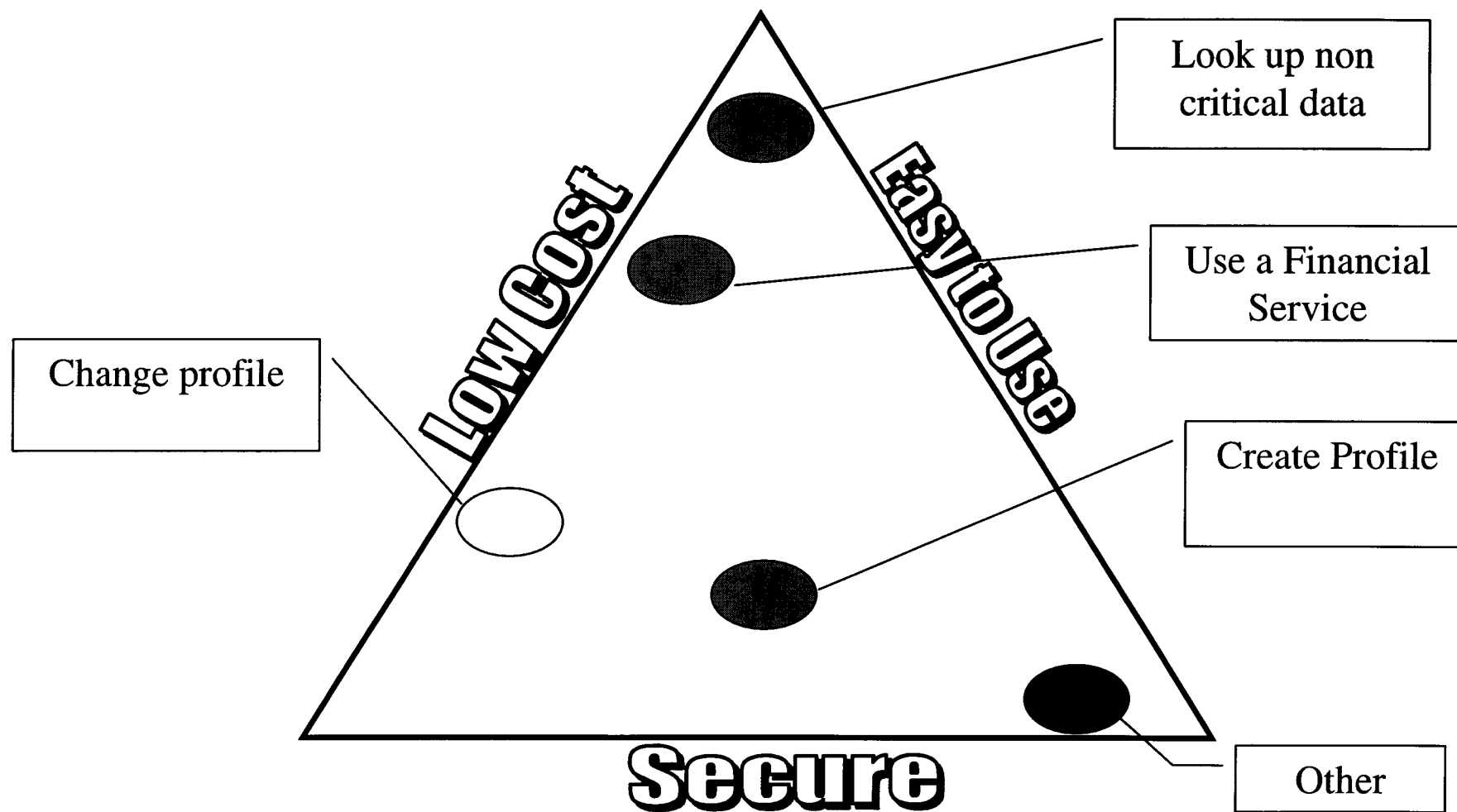
# **Services / Operators**

**...operationally doable**

- **Identity verification\* / Credential enrollment services (Registration Authority)**
  - **Banks / USPS**
- **Identity Issuance services**
- **Identity Authentication Service**
- **Consumer service**
- **Dispute resolution service**



# Security Goal



# Passport Trust Models

- **Centralized vs. Decentralized**
- **Single or multiple ID issuers**
- **High / Medium / Low assurance**
  - **Authentication**
  - **Identification**

# The Passport Service

## ...eAuthentication experience

- **Consumer interaction**
- **Legal / Regulatory interaction**
  - Privacy law / COPA
  - EU Safe Harbor
- **Security Experience**
  - Relying Party
  - Tool / product provider
  - Personnel
  - Service user
  - Service Providers
  - Data Providers
- **Operational Experience**
  - Scale
  - Reporting / Logging

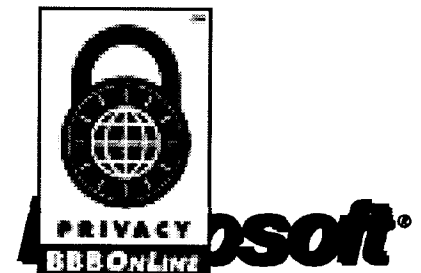
# The Passport Service

- **Platform for Web services – offers authentication of user identity**
  - PUID – unique, global, static identifier
  - Profile – (optional) demographic and selected personal information
  - Scope of sharing – set of sites with common TOU and privacy policy
- **Applications**
  - Primarily – Consumer access to Hotmail and MSN.COM
  - MSN Messenger Connect – Managed Instant Messaging for enterprises
  - Microsoft Developer Network (MSDN)
  - A growing number of 3<sup>rd</sup> parties
- **Namespaces**
  - 300,000,000 active identities
  - 90% in msn.com, hotmail.com and hosted namespaces
  - 10% in other namespaces (“EASI” – Email as Sign-In)
- **Passport facilities separate from MSN**
  - distinct TOU and Privacy Policy
  - separate data center cages and operations staff

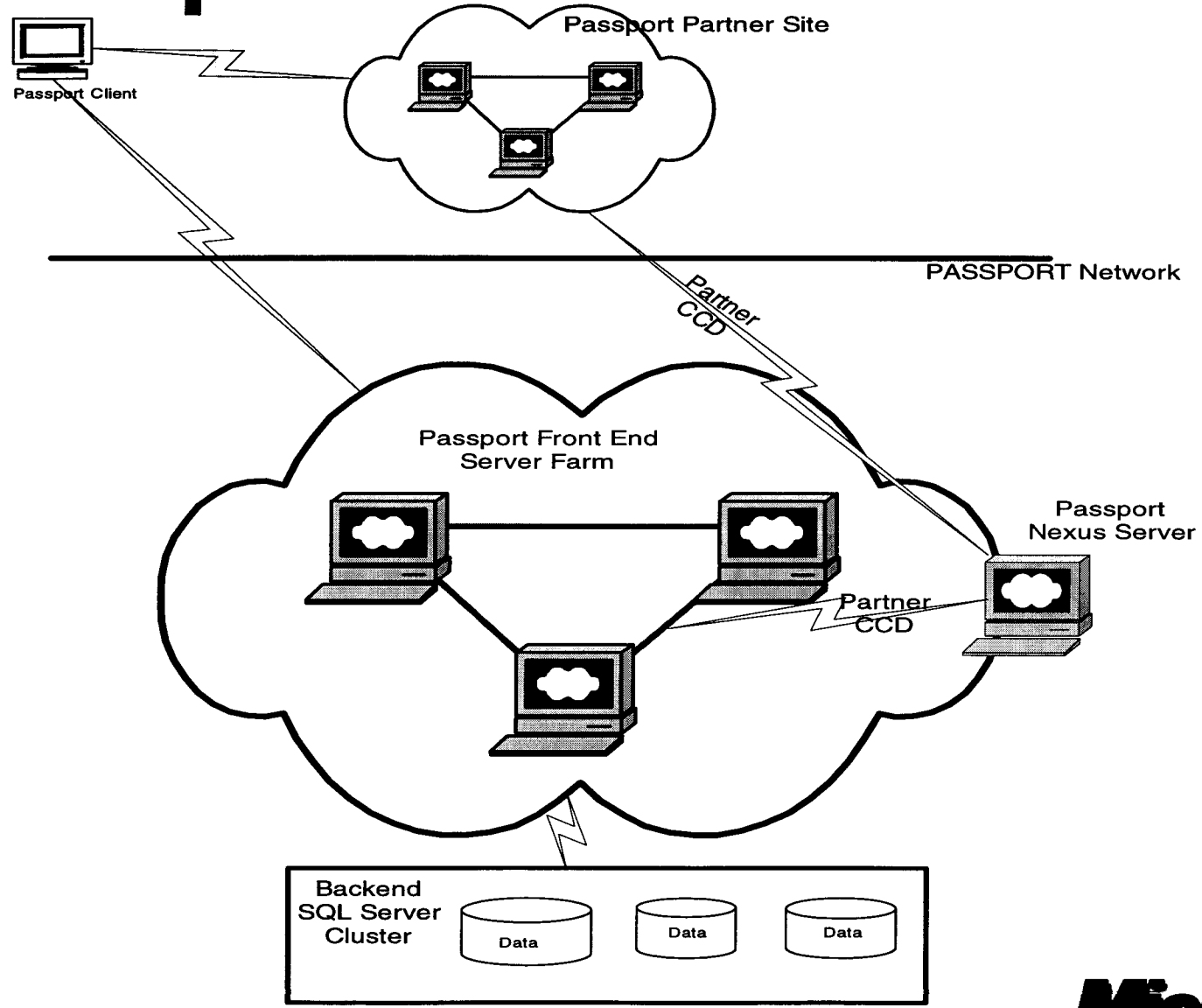
# Privacy Policy

- **Critical success factor: trusted data management**
  - Passport does not mine, sell, rent, or market Passport data
  - Passport does not allow secondary use of Passport data by Microsoft or anyone else
  - Passport facilities not shared
- **Focus is on consumer empowerment**
  - Easy user management of consent/permissions
  - Passport contract requires participating site to post their privacy policy and to support P3P
  - We support E.U. Safe Harbor

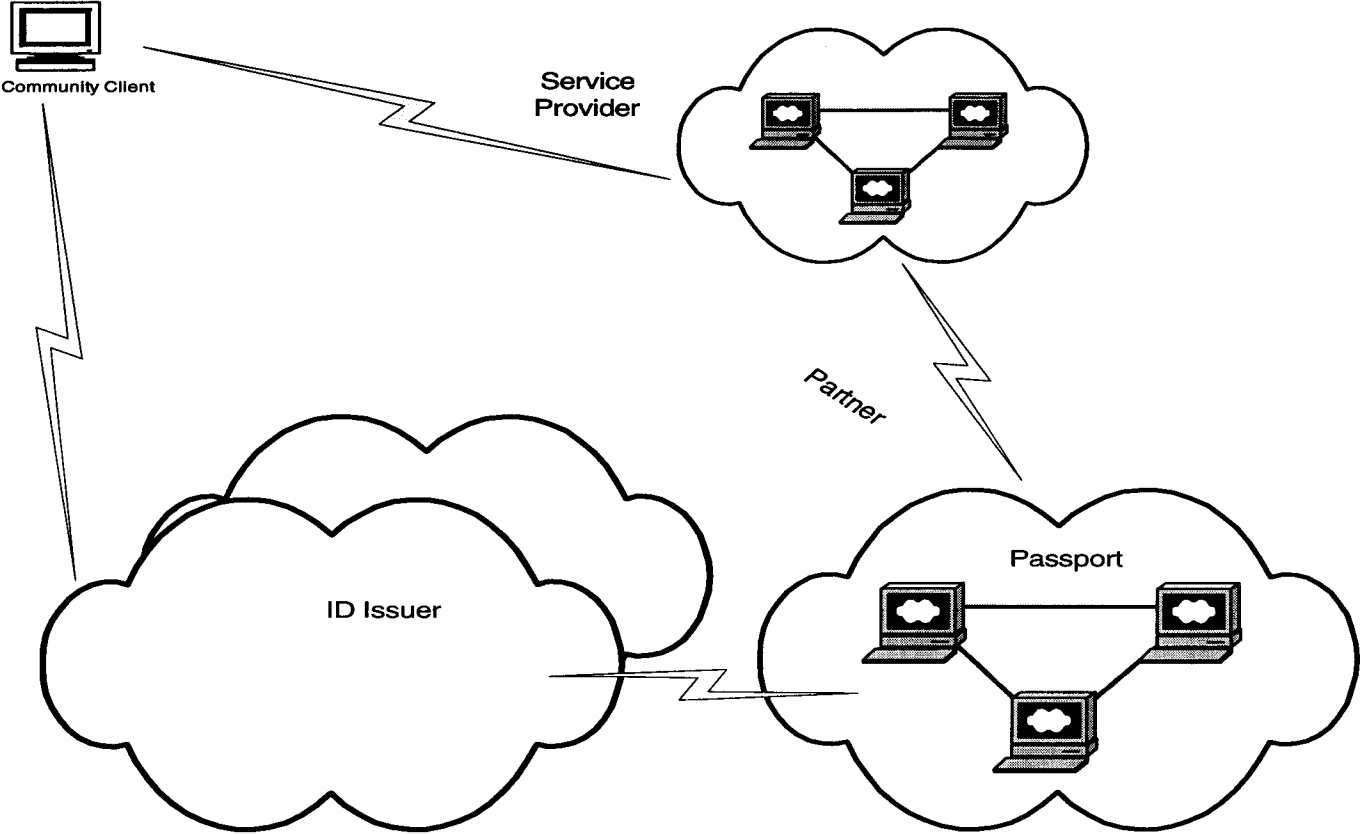
13



# Passport Architecture



# Passport Architecture



# Security

**...Deter, Deny, Detect, Defuse**

- **Protected data centers**
  - **Physical access controls**
  - **User information stored on servers that are not directly connected to the Internet**
- **Secure Coding practices**
- **Comprehensive use of data and session encryption**
- **Perimeter protection and service monitoring / IDS / Firewalls / Log Analysis**
- **Audited Operational framework**
- **Secure Operational procedures**

**Microsoft®**



# Future Exploration

...stronger auth and privacy options

- **Cert based auth**
- **Dual password**
- **One time password**
- **Phone based Authentication**
- **Multiple Issuers of ID**
- **Multiple Authentication services in 'Federation'**

# Q & A

# Authentication vs. Authorization



**Authentication is the process of uniquely and reliably identifying a user**

**Cf. Authorization, determining what a user can do**



- Sites, devices, networks, and applications need a way to provide a secure, customized experience
- A reliable authentication mechanism is important in any electronic service relationship and to ensure the integrity of any transaction