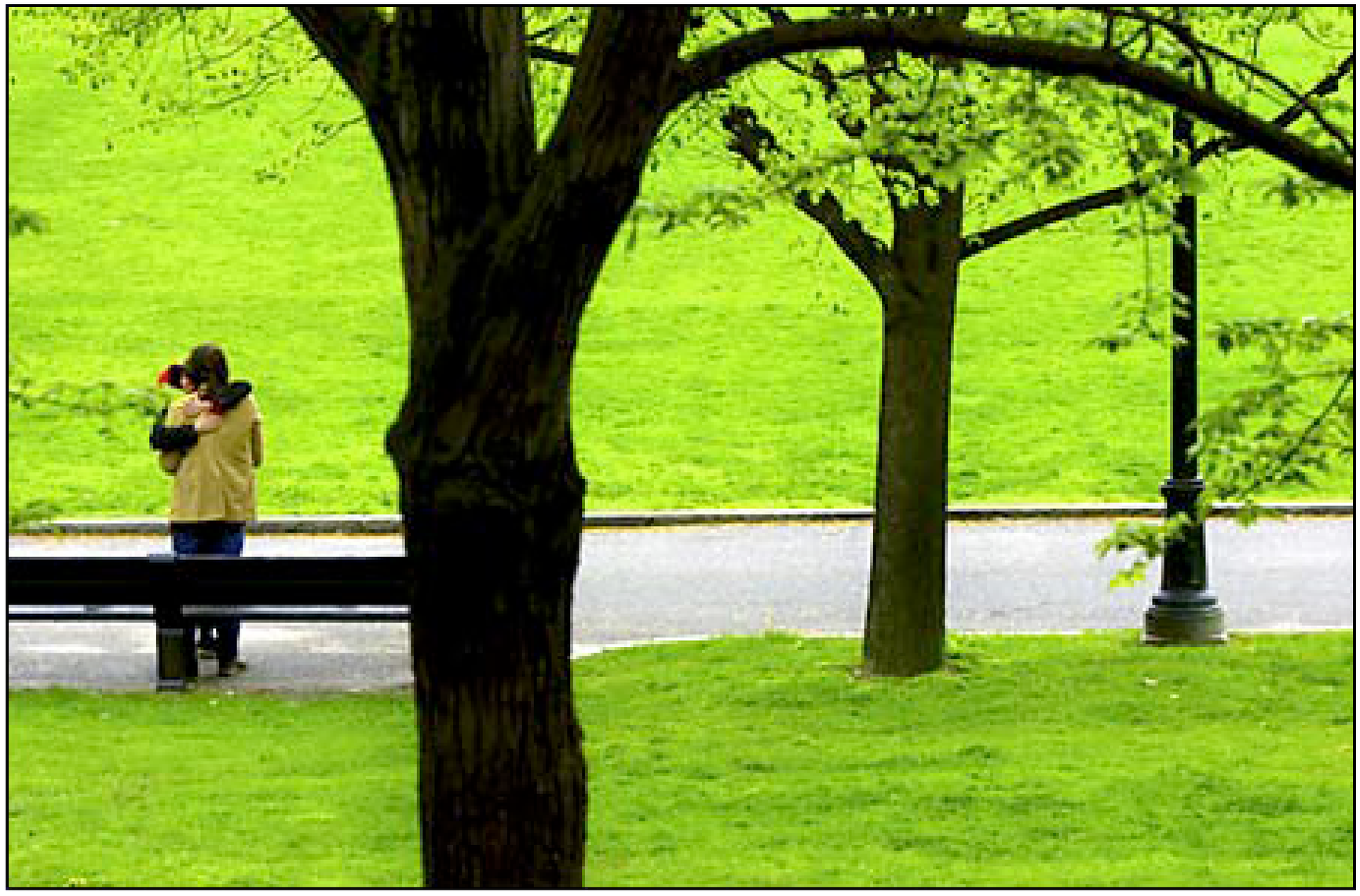
UTORauth: Middleware for the Masses

Russell Sutherland
CNS, University of Toronto
russell.sutherland@utoronto.ca
+1.416.978.0470

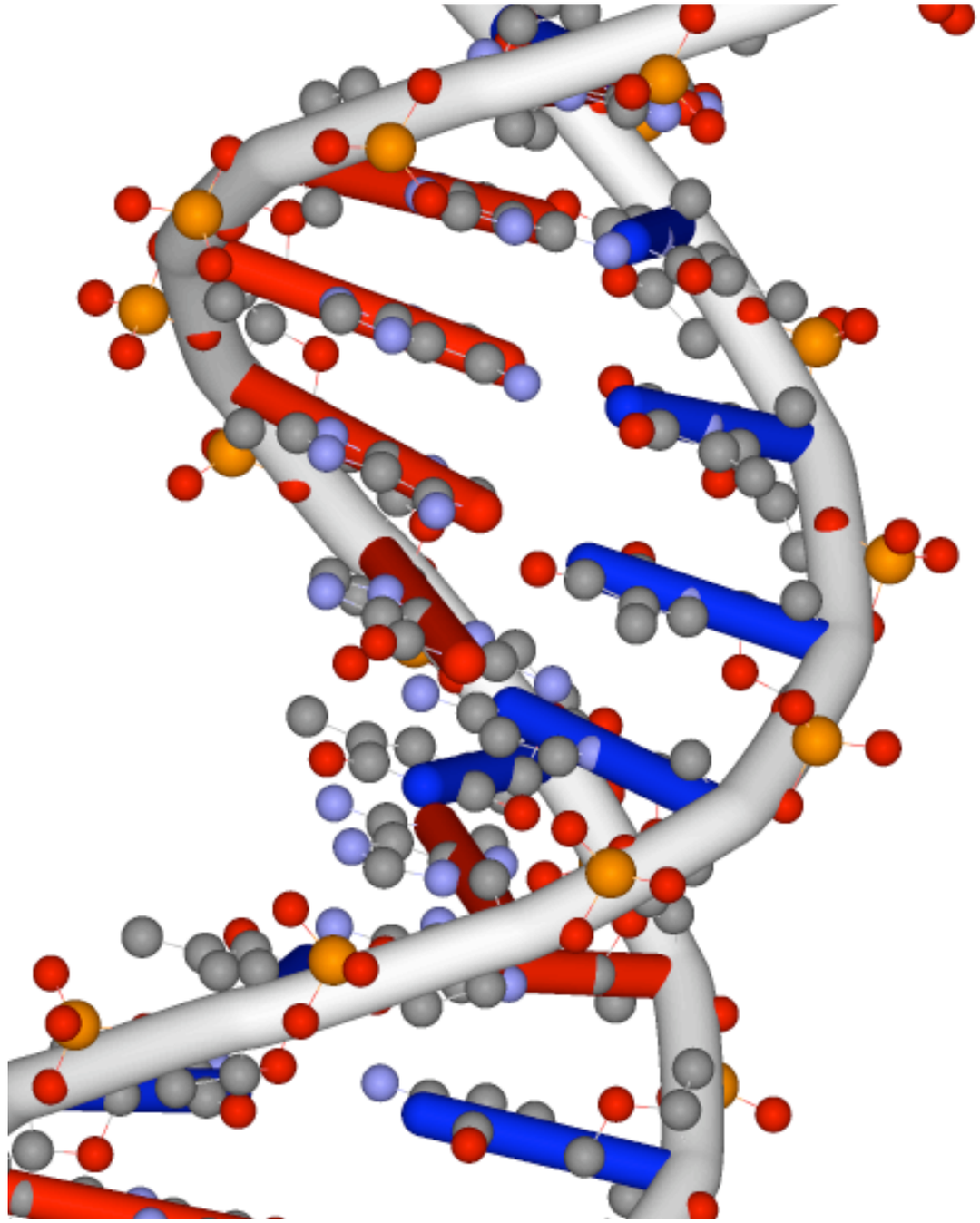
URL for Tree Huggers



http://madhaus.cns.utoronto.ca/~russ/canheit2006.pdf

Identification

Who am I?



Identification

Am I Unique?

Identification

What me worry?

Identities and Identifier Creation Elements

- Raw Materials
    - Name

Alfred E. Newman

Identities and Identifier Creation Elements

- Raw Materials
    - Date of Birth

1954-03-11

Identities and Identifier Creation Elements

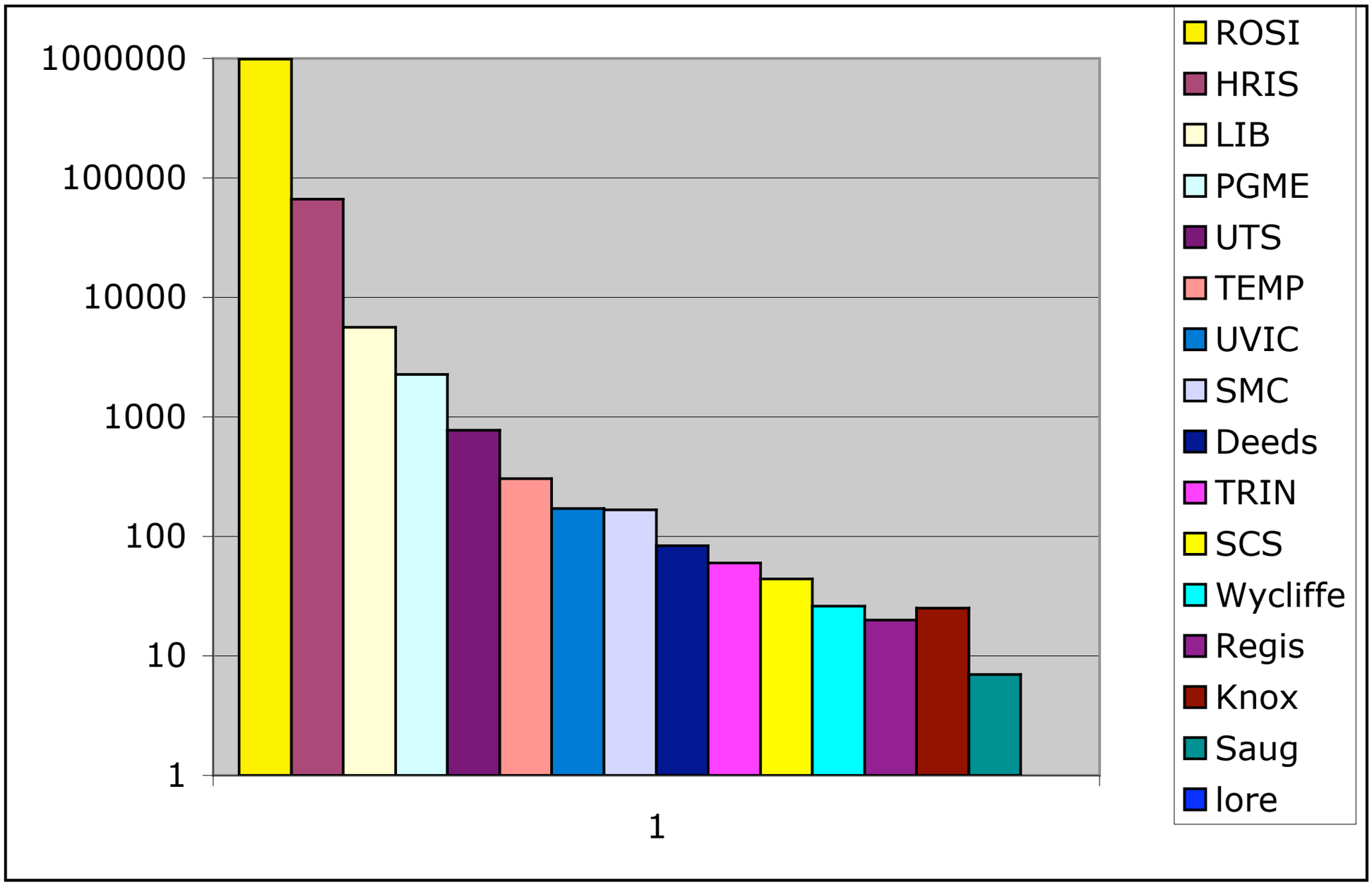
- Raw Materials
    - Sex and SIN

M 722-231-122

UTORauth ID Data: Sources

- Student Information Systems
- Human Resources Information Systems
- Federated Colleges (5)
- Teaching Hospitals (12)
- Miscellaneous (8)

UTORauth ID Data: Sources



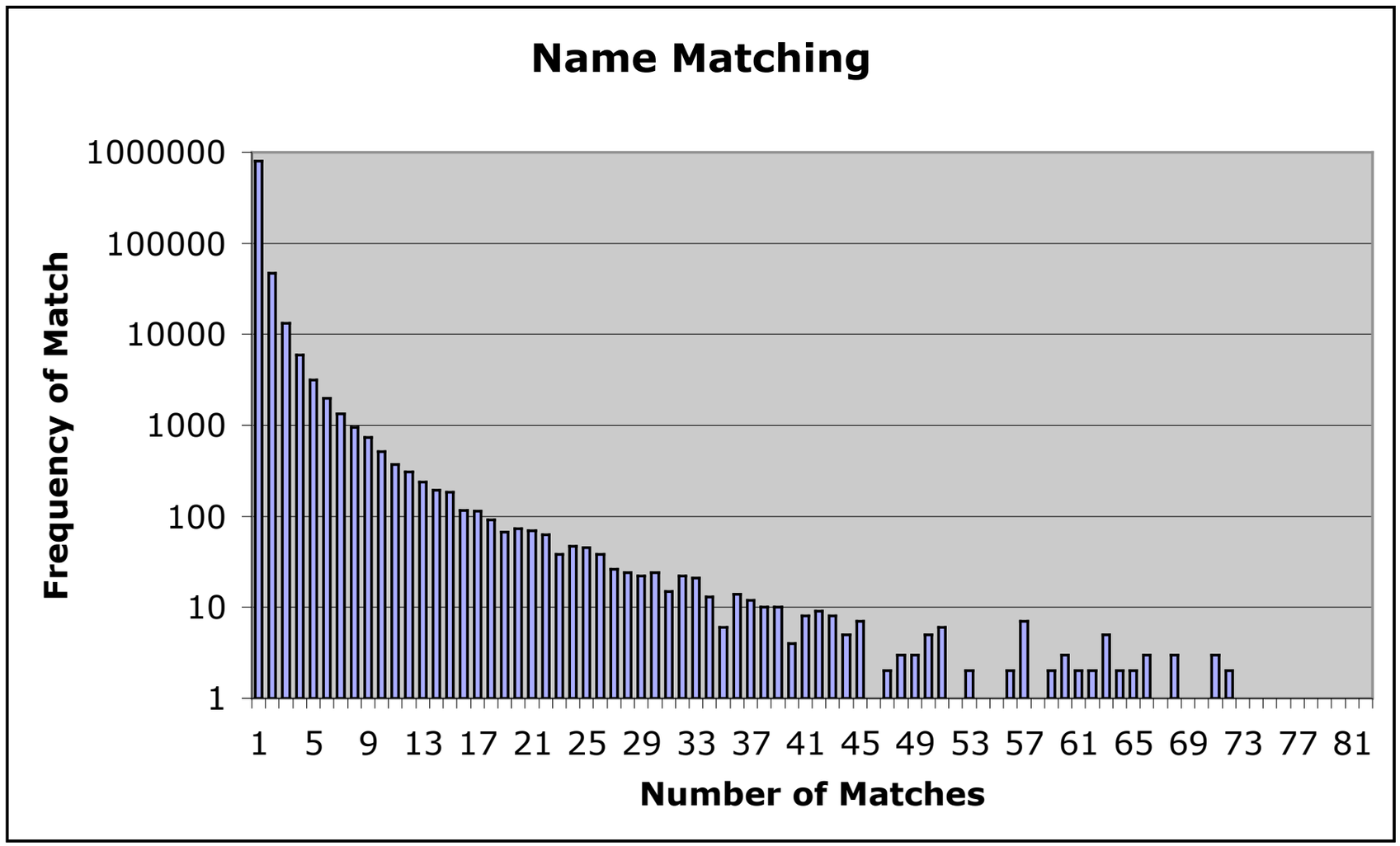
UTORauth ID Data: Merging and Matching

- Basis of **1.05** M records
- Fname + Sname + DoB + SIN
    - **6** non-unique records
- Fname + Sname + DoB
    - **31** non-unique records
- Sex is useless!

UTORauth ID Data: Merging and Matching

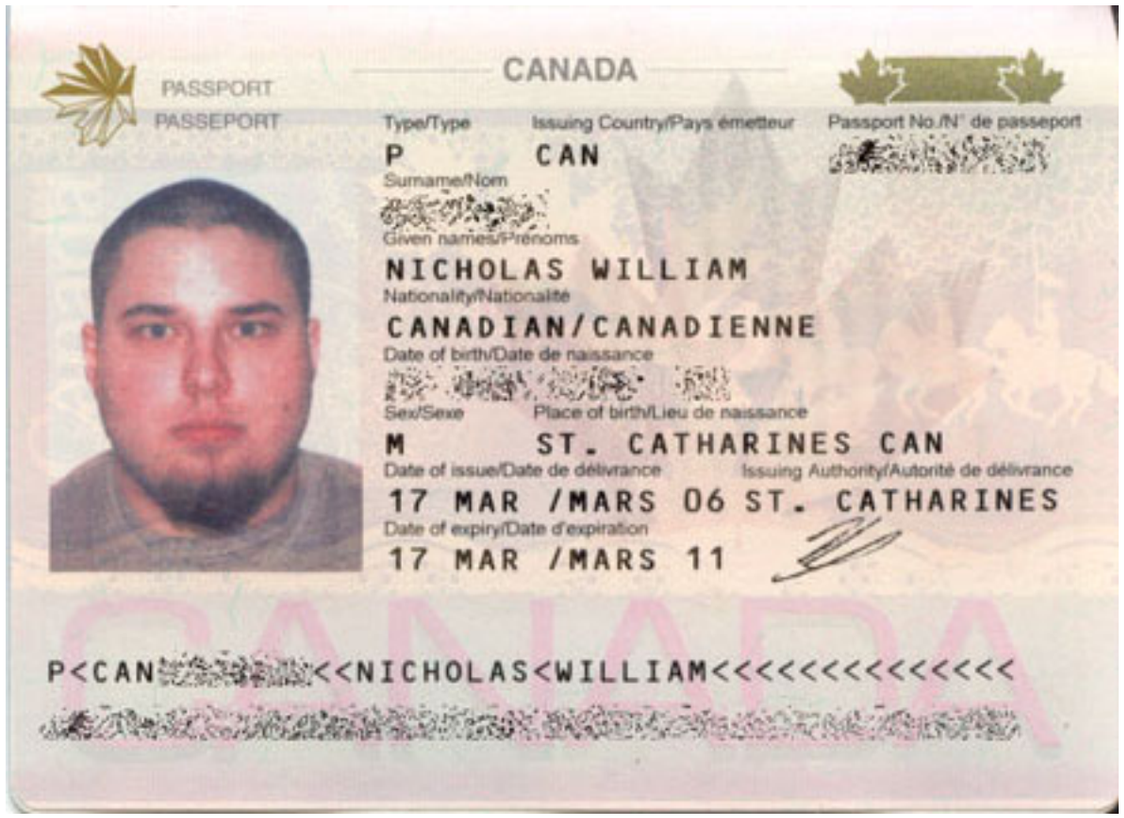
- Basis of 1.05 M records

- Fname + Sname



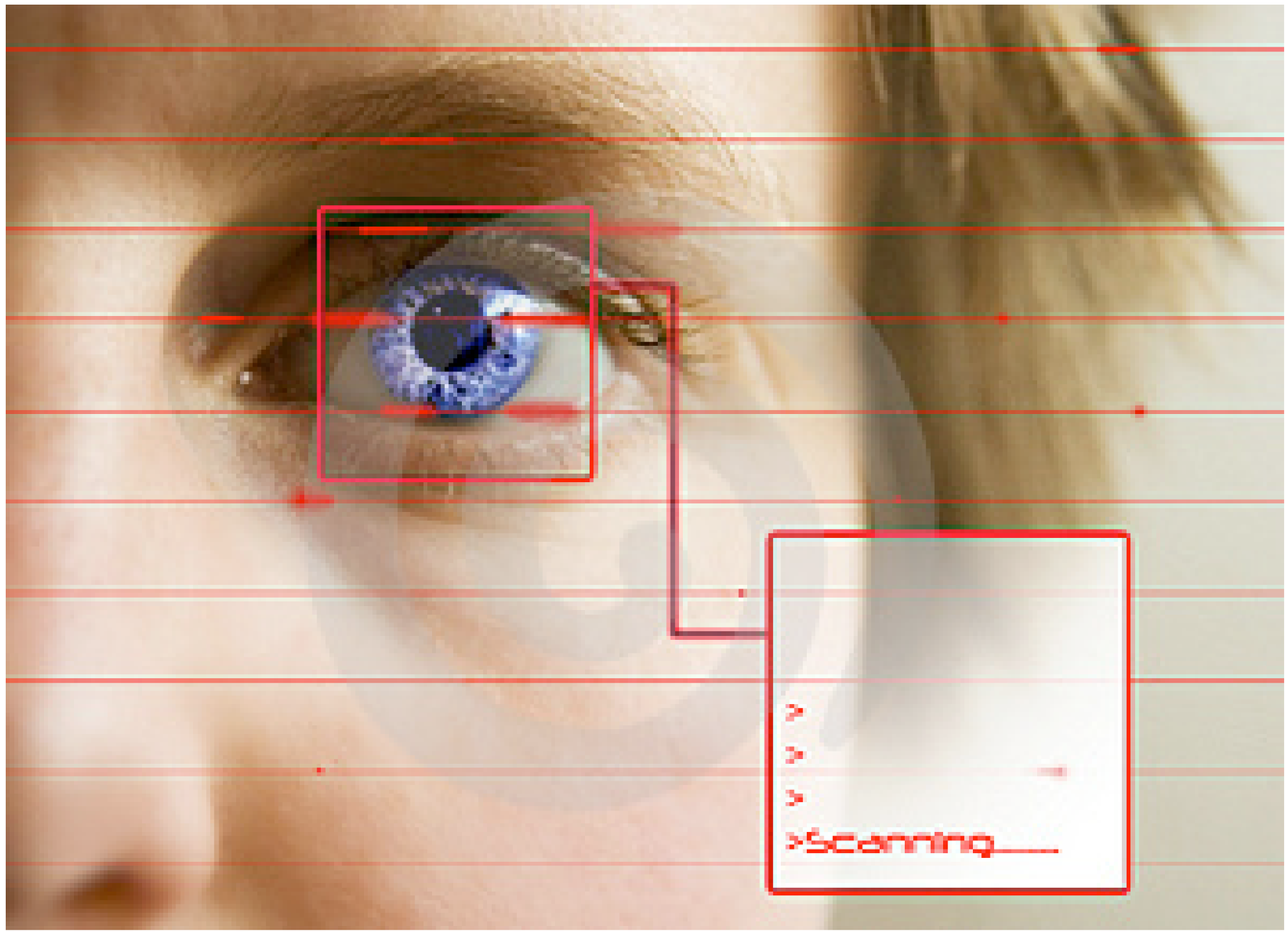
Authentication: Proof of Identity

- Canadian e-Passport



Authentication: Proof of Identity

- Biometric Scanning
- CANPASS



Authentication: Proof of Identity

- Institutional ID Card
- UofT == TCard

Stu/Staff Num

UTORid

BarCode/LibNum

Authentication: Proof of Identity

- Username and Password
- Semi Private + Private
- Basic Level of Remote Authentication

Identifiers

- Standard Reference Document

  - Identifiers, Authentication, and Directories:
    Best Practices for Higher Education
    http://middleware.internet2.edu/internet2-mi-best-practices-00.html

- UTORauth creates two main user IDs:

  - Universal Identifier UTID

  - Network Identifier UTORid

UTID Properties

- **U**niversity of **T**oronto Unique **ID**entifier
- 10 digit internal identifier
  - 9 + 1 check digit
- Not known by individual
- Example:

1 001 327 805

UTORid Properties

- **U**niversity of **T**oronto Network **ID**entifier
- 8 (or less) alphanumeric string
- Examples:
  - **vernejul smithk35 newmana**
- Known by the individual
- Derived from person’s name for easy of use [lucency]
- Used by all UTORauth Network Applications

UTORid Generation and Issuance

- Students
  - TCard Office: TCard + UTORid + SAK + Info. sheet
- Central HR Staff (Faculty and Admin)
  - Local Business Officer: UTORid + SAK (opt) + Info. sheet
- Non HR Staff (Faculty and Admin)
  - SSL Web based upload/download of ID data

UTORid Generation and Issuance

- Temporary/Contractual Staff [fixed termination date]
    - TCard Office: TCard + UTORid + SAK + Info. Sheet
- Sponsored Individuals
    - time less than 7 days
    - Any staff or faculty with a UTORid can generate a sponsored UTORid
    - limited utility

UTORid Activation

- UTORids are generated with a one time password
- SAK == Secret Activation Key
- Activation involves:
  - choosing an institutional email address
  - choosing a UTORid password
  - performed via a secure https web session

UTORauth Authentication

- Uses Kerberos [*http://web.mit.edu/kerberos/*] as the back-end authentication technology

- All Web Applications use Web Login
  [aka Pubcookie *http://www.pubcookie.org/*]

- Authentication transparent to the WWW application

- A re-direct is performed to the institutional login server:

  - https://weblogin.utoronto.ca

- Works with: Apache 1.3, 2.0 and IIS 4.0

UTORauth Authentication: Single Sign On

- All Web Applications use Web Login
  [aka Pubcookie *http://www.pubcookie.org/*]
  - A single login page can authenticate for any utoronto.ca web service.
  - Input your UTORid and password once only to access several services.
  - Uses web browser's cookies to hold authentication data.
  - Exit browser to remove these special cookies from the browser cache.

Authentication

- Has been integrated with
  - Windows workstation authentication against a Domain Controller
  - Unix/Linux PAM login

Authorization

- What privileges do I have as an authenticated user?
- All UTORids have a long list of associated state information
- Applications access this state information to make local decisions

Authorization: UTORable

- A central repository of information relating to the state and properties of persons
    - Is_student
    - Program of Study
    - Barcode
    - Email Address
- Referenced by UTORid or UTID
- Created by unifying and merging University data

Authorization: UTORable Policies

- Access limited to registered clients
  - i.e. UofT Departments etc.
- No access to end users
- Clients
  - have limited access
  - create their own rules for their own users
    - e.g enrolled in MAT133Y and ! FSL221

Authorization: UTORable Data Access

- Data available on a batch basis
  - Rules determined by client
  - Delivered on a daily basis
    - protocol: ftp, ssh, scp
- Data available on an interactive basis
  - OpenLDAP
  - APIs are readily available for PHP/Perl/C etc.

Usage

- Over 15 Large applications
    - Help Desk
    - Engineering Lab Access
    - TCard Office
    - PAF Workstations
    - LMS System
- 2 or 3 new implementations per month

Documentation

- General
    - http://www.utorauth.utoronto.ca/
- Web Login Authentication
    - http://www.utorauth.utoronto.ca/?page=weblogin
- UTORable
    - http://www.utorauth.utoronto.ca/?page=ldap

Conclusion: Three Keys to Success in Middleware