The Three Toes of UTOR(sl)auth

Russell Sutherland
University of Toronto
Computer and Networking Services

$Date: 2003/05/15 13:09:42 $

URLs for the Tree Huggers

- http://madhaus.cns.utoronto.ca/~russ/techknowfile/
- http://madhaus.cns.utoronto.ca/~russ/utorauth.pdf

Definitions

- Identification
  - Who you are
  - "I am Sam"
- Authentication
  - Proves you are who you say you are
  - --> "I am Sam"
  - <-- What is the full name of Dr. Seuss?
  - --> "Theodor Seuss Geisel"
- Authorization
  - What you can do:
  - "Sam is allowed to read the digital copy of Green Eggs and Ham"

The Identification System

- Ensures a common unique identifier for each UofT community member
- Collects basic identity data from authoritative sources
  - SIS
  - HRIS
- Issues a unique UTID (UofT IDentifier)
- UTID Format: 10 digit number or 11 Digit string
  - 9081726354
  - 90817-26354
- Unknown to the person
- Known and used by UofT systems as a unique identifier
- Used as a basis to generate other identifiers:
  - barcode
  - UTORid
- Accepts limited queries from other systems

The Authentication System

- Implementation is based on Kerberos
- Key Distribution Centers (KDC) will be available to all clients
- WWW browser based authentication will use PubCookie
- Kerberos credentials are based on
  - a principal or login ID
  - a corresponding passphrase
- The UTORid will be used as the principal

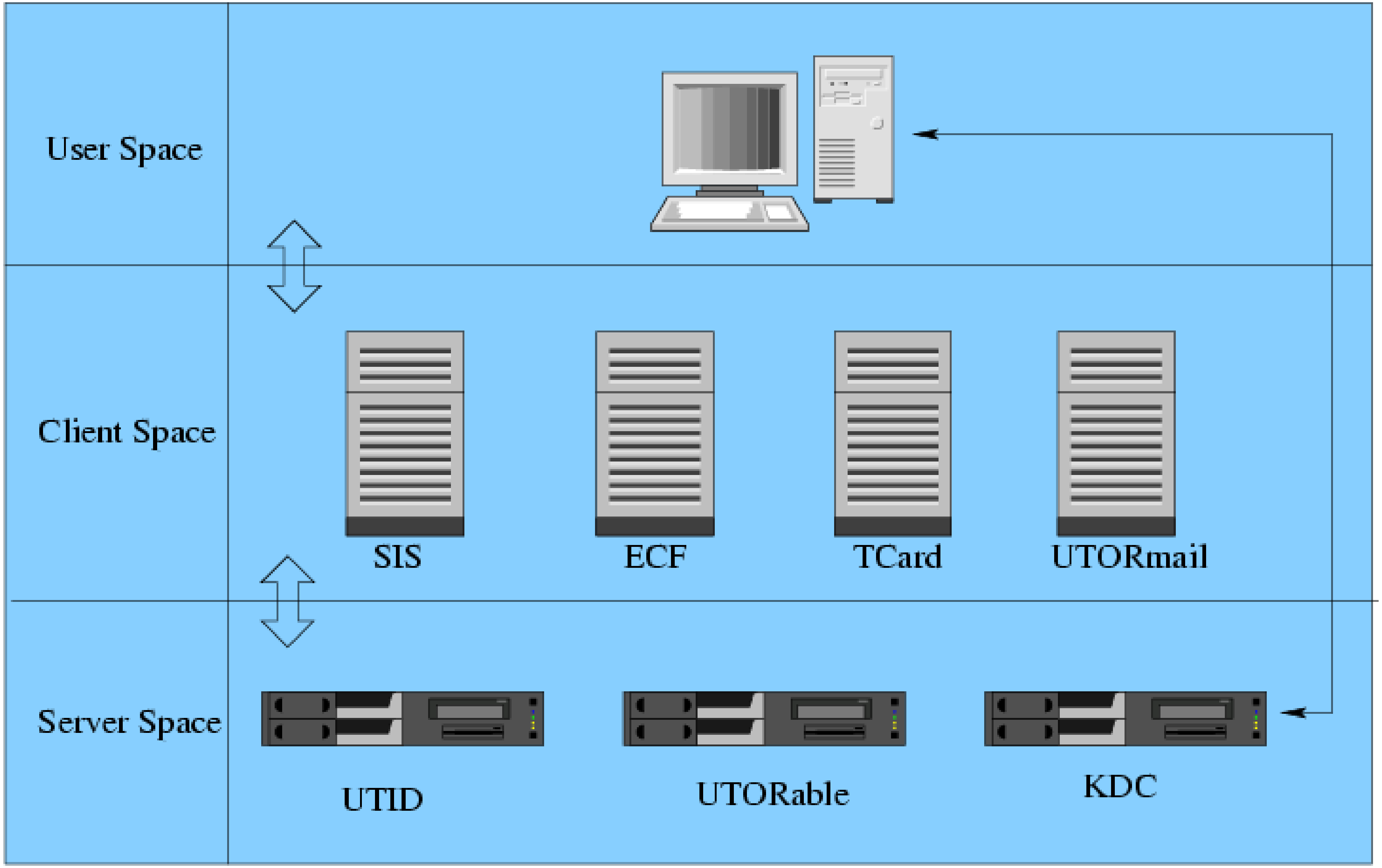
Kerberos Fundamentals

- Stable and reliable authentication technology (MIT, 1988)
- Uses secret key cryptography
- Based on a 3rd party authentication agent (KDC)
- No passphrases transmitted over the network
- Requires both client and service to speak to the KDC
- Adopted by Microsoft and available for Win2k

Authorization System: UTORable

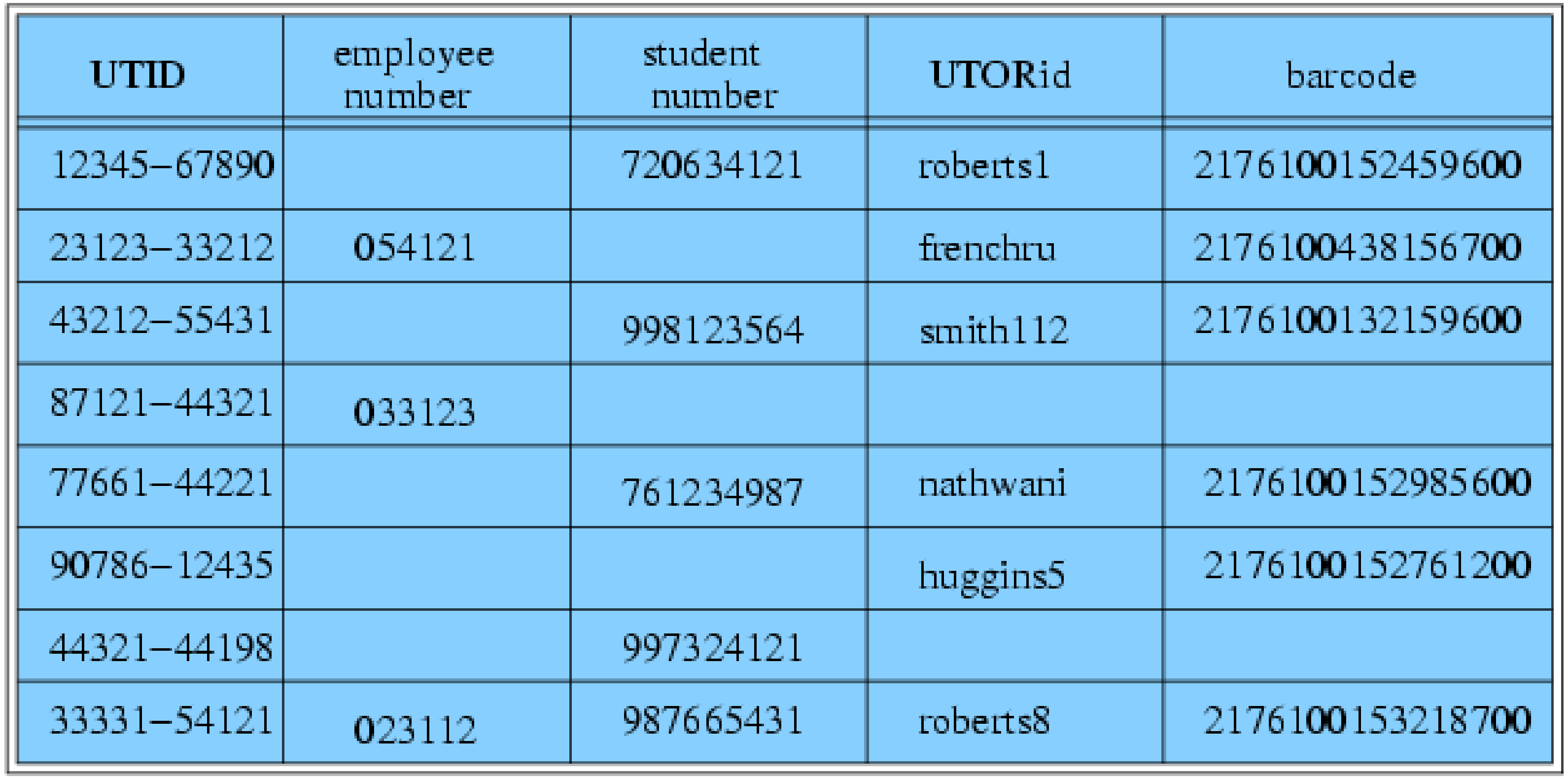
- Provides a central directory of information for UofT staff/faculty/students
- Accessible to registered clients ***
- Level of access is granted on the basis of the client service requirements
- Clients:
  - Offer services to end users
  - Set their own rules and policies
- Data available on a batch or an interactive basis
  - Interactive -> LDAP
  - Batch -> FTP/SSH
- No end user can access UTORable directly

UTORauth Architecture



UTORable Contents: ID Mapping

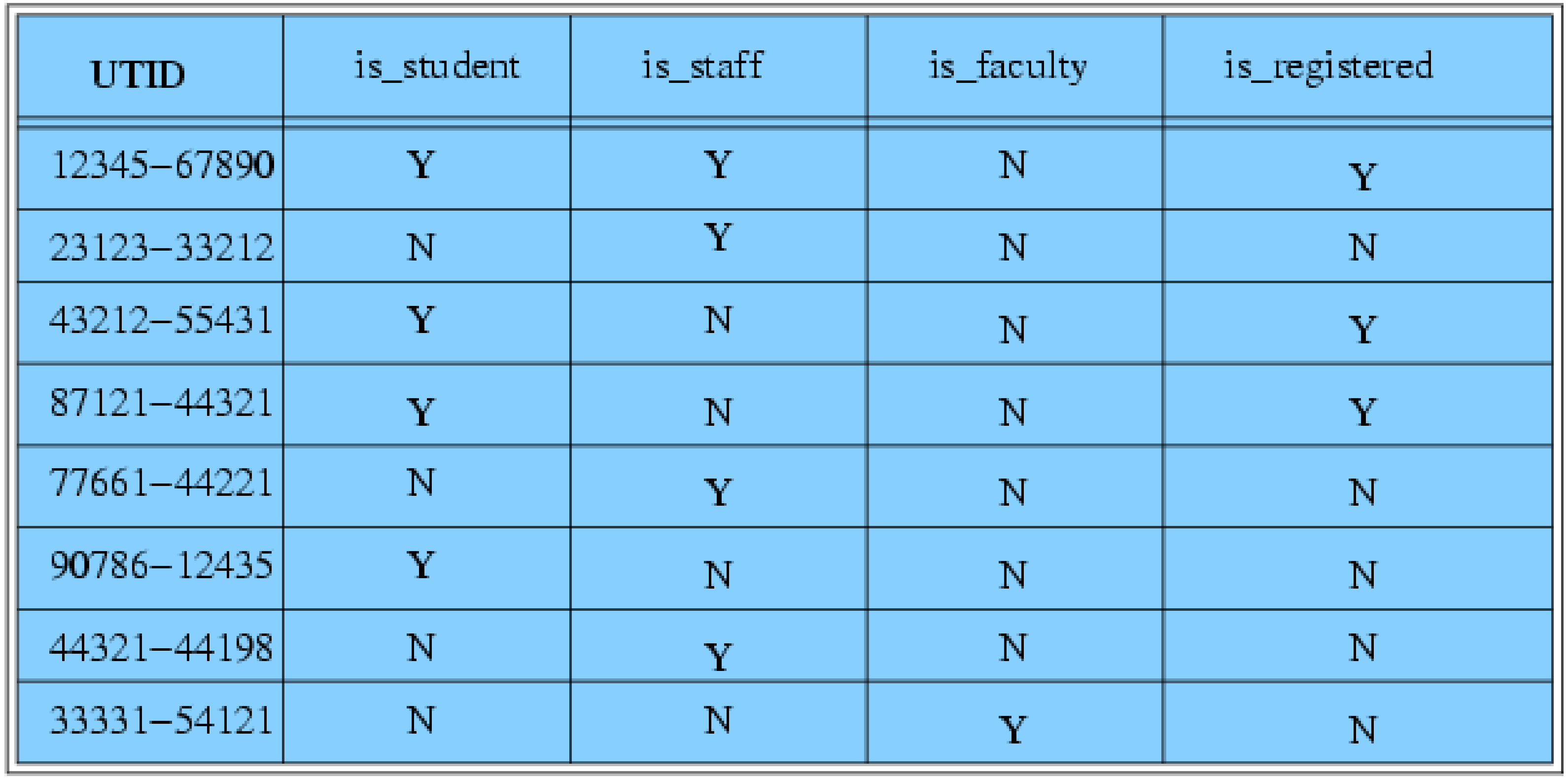
- Current Identifiers
  - UTID
  - UTORid
  - barcode
  - student number
  - employee number



UTID	employee number	student number	UTORid	barcode
12345–67890		720634121	roberts1	217610015245960
23123–33212	054121		frenchru	217610043815670
43212–55431		998123564	smith112	217610013215960
87121–44321	033123			
77661–44221		761234987	nathwani	217610015298560
90786–12435			huggins5	217610015276120
44321–44198		997324121		
33331–54121	023112	987665431	roberts8	217610015321870

UTORable Contents: State Info.

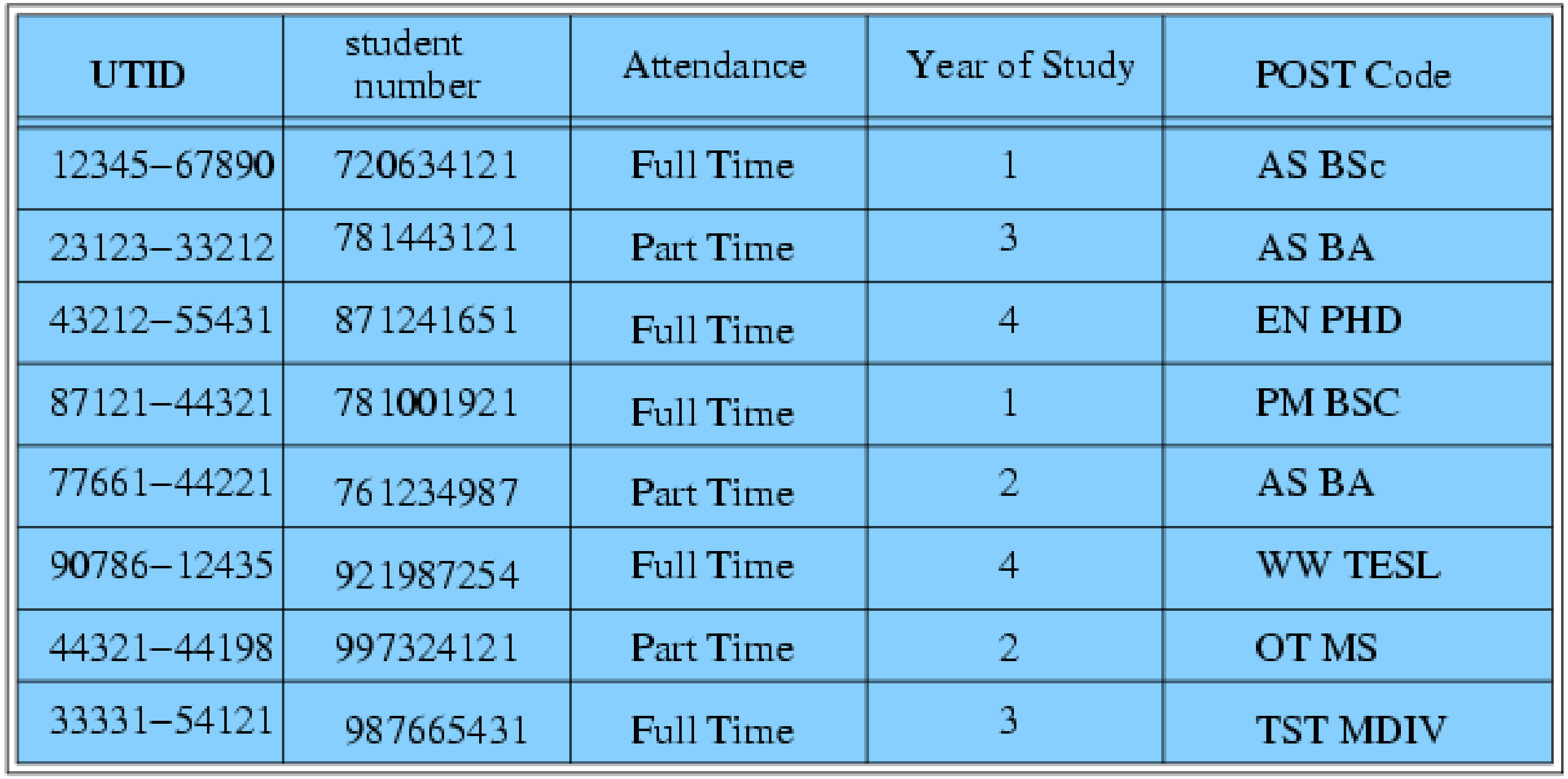
- Status
  - is_staff
  - is_faculty
  - is_student
    - is_registered
    - is_invited



UTID	is_student	is_staff	is_faculty	is_registered
12345–67890	Y	Y	N	Y
23123–33212	N	Y	N	N
43212–55431	Y	N	N	Y
87121–44321	Y	N	N	Y
77661–44221	N	Y	N	N
90786–12435	Y	N	N	N
44321–44198	N	Y	N	N
33331–54121	N	N	Y	N

UTORable Contents: Student Info.

- Mirror of ROSI data
  - Programme of Study
  - Session
  - Courses
  - Registration Code
  - Bags of other information



UTID	student number	Attendance	Year of Study	POST Code
12345–67890	720634121	Full Time	1	AS BSc
23123–33212	781443121	Part Time	3	AS BA
43212–55431	871241651	Full Time	4	EN PHD
87121–44321	781001921	Full Time	1	PM BSC
77661–44221	761234987	Part Time	2	AS BA
90786–12435	921987254	Full Time	4	WW TESL
44321–44198	997324121	Part Time	2	OT MS
33331–54121	987665431	Full Time	3	TST MDIV

Application One: The TCard Office

- Function
  - Issues a TCard for Sam
  - Create a personalized UTORid information sheet which includes a Secret Activation Key (SAK)

TCard Chronological Info Trail

- Sam applies to OUAC
- Sam’s identity info is transferred OUAC -> SIS -> UTORauth
- Sam’s UTID is generated and passed back to SIS
- Registrar offers Sam admission
- SIS passes acceptance data to UTORauth
- Sam’s barcode, UTORid and activation code generated
- Sam arrives at TCard office and presents credentials:

  photoID + letter of offer
- TCard queries UTORable with the Sam’s stunum
- UTORable returns all info for the TCard:

  Name + Programme of Study + barcode + UTORid + SAK
- Populated TCard is issued along with a separate UTORid information/activation page which includes SAM’s SAK

Application Two: The PAFs

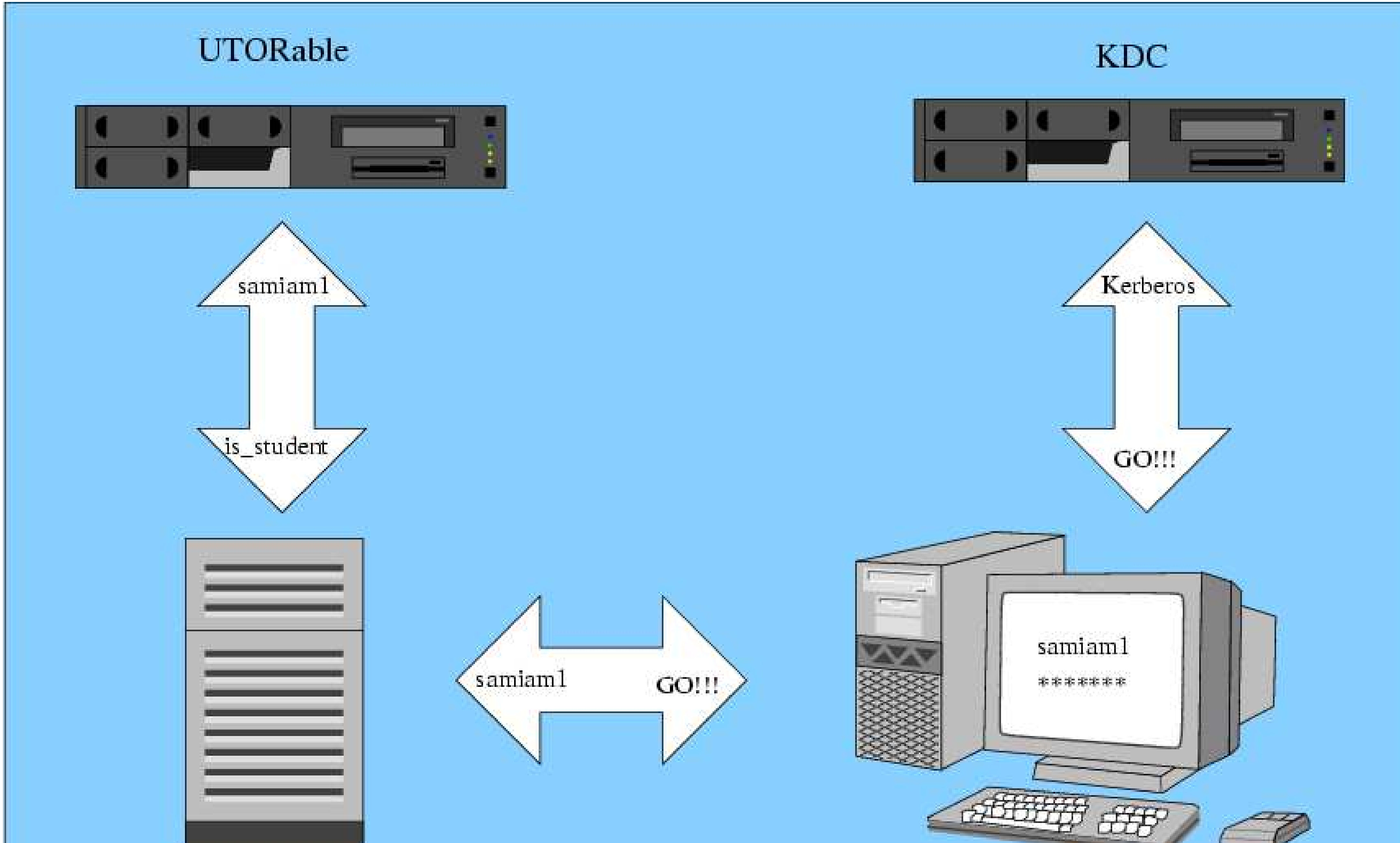
(PAF == Public Access Facility)

- Function:
  - To control access to the PAF workstations
    - who
    - for how long
  - To collect accounting data for each session

PAF Chronological Info Trail

- UTORid/passphrase entered to workstation login screen
- Workstation authenticates via Kerberos
  - failure == no access
- Workstation passes UTORid to PAF accounting server
- Accounting server queries UTORauth for the status of the UTORid
  - is_faculty -> access
  - is_staff   -> access
  - is_student -> access
- Accounting server records user session data

PAF System Schematic



UTORid Features

- One person ... one UTORid
- Mnemonic in form: samiam1
- Has an associated pass phrase: iLuvSuess!
- Chief network identifier for accessing current and future campus services

UTORid Assignment + Activation

- New Students
  - TCard Office
    - credentials + letter of invitation
    - UTORid printed on TCard
    - Secret Activation Key distributed
    - UTORid WWW site for activation
- Existing Students, Faculty and Staff
  - Prerequistes
    - barcode
    - stunum/personel number
  - UTORid WWW site
    - www.utorid.utoronto.ca