Anonymous Course Evaluations at Universities: The Patras University Pilot

Yannis Stamatiou,
Computer Technology Institute (CTI) & Press –
"Diophantus"

ABC4Trust Information Day,
29 September, Athens, 2014

Agenda

The Computer Technology Institute (CTI) at a glance

CTI's new role towards the reform of the Greek educational system

The Greek School Network: CTI's vehicle towards educational reform in Greece

ABC4Trust University Course Evaluation pilot: CTI's vehicle for building privacy preserving ePartipation in Greece

CTI at a crossroad: its key role in reforming the Greek educational system and eGovernance

Identification

The **Research Academic Computer Technology Institute** is a **research** and **development** organization.

It is a **non profit** legal entity, **supervised** by the **Ministry of Education, Lifelong Learning and Religious Affairs,** enjoying financial and administrative independence.

It was established in 1985, in Patras where its head offices are located.

Its statutory was updated in May 2, 2001, according to the Law 2909/01. This updating was a strategic choice of the Ministry of Education and Religious Affairs in order to use the organization's activity and competitive advantage mainly for the purposes of the Information Society.

Goals

To conduct basic and applied research in H/W & S/W and network technologies, and the socio-economic impact of Information Society.

To design and develop products and services.

To support all forms of education and **training** in Information & Communication Technologies.

To develop technology and transfer know how.

To provide the Ministry of Education and Religious Affairs, the public sector, any natural or legal entity and social institution with **consulting, planning and administration services** in fields concerning the Information Society.

The Information Society Sectors are the organization's conveying mechanisms of know-how, in turn supporting the Hellenic State's devolvement into the Information Society.

The Sectors are coordinated by the **Board of Executives**

The Sectors are:

- **Educational Technology Sector**
- Networking Technologies Sector
- E-Government Sector
- Center of Telematics & Applications for regional development
- **Further Education & Training Sector**
- Strategic & Development Policy Sector
- Computing & Networking Systems Security Sector

Information Society Sector

Yannis Stamatiou, CTI

Infrastructure

CTI is situated In a privately owned building complex, at the University of Patras Campus. It covers a total area of 4.430 m^2.
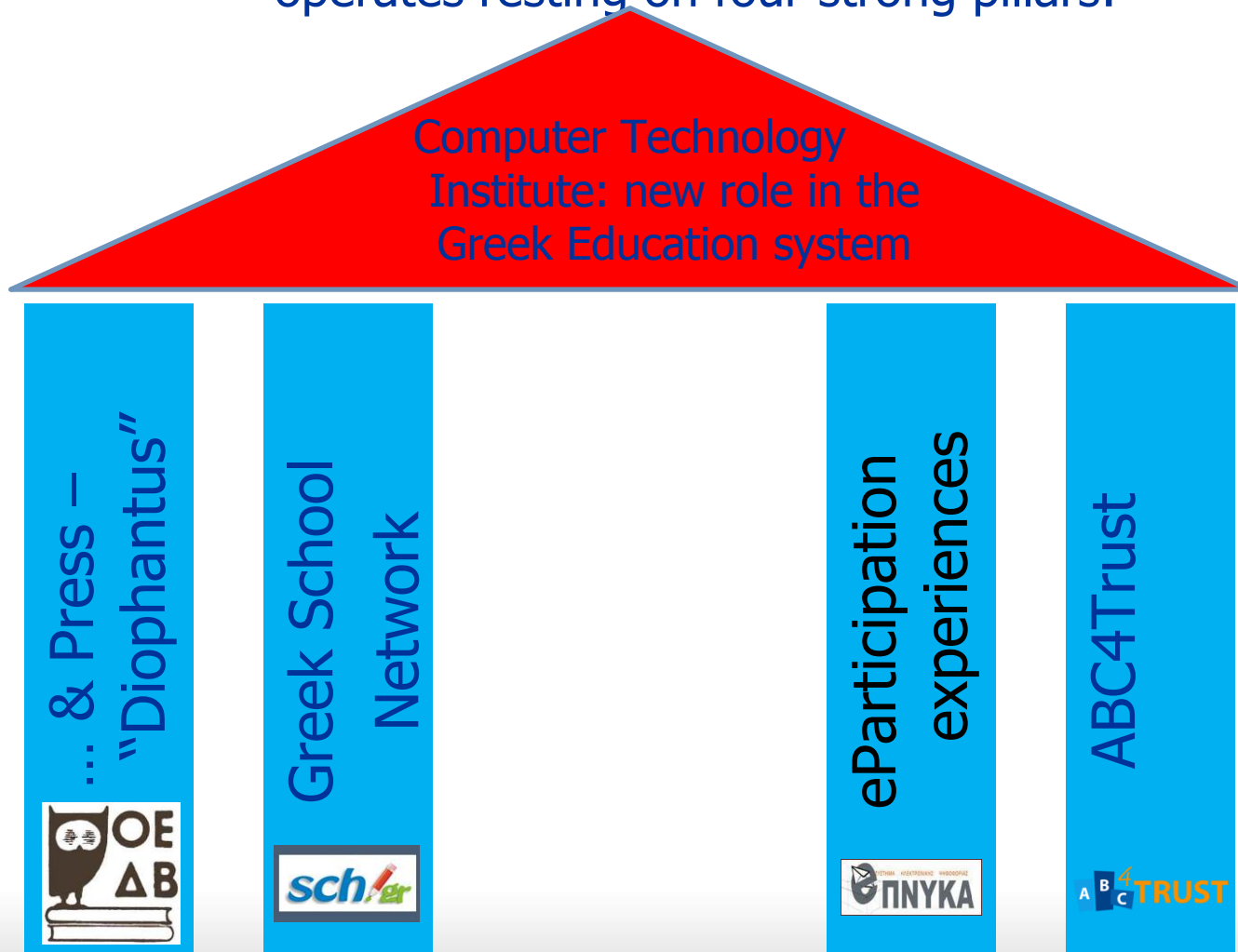
Also, in additional offices in Athens

CTI's new status: rests on four pillars

Today, CTI has a new role as a governmental educational agency and operates resting on four strong pillars:

Computer Technology Institute: new role in the Greek Education system

... & Press – "Diophantus"

Greek School Network

eParticipation experiences

ABC4Trust

Yannis Stamatiou, CTI

The institute's rebirth and new responsibilities

- [ ] The start of the year 2011 saw a rebirth of CTI: law was passed that enhanced CTI's responsibilities to embrace more strongly the Greek Educational Sector.

- [ ] CTI absorbed the state's official publisher of educational books and assumed its responsibilities

- [ ] CTI is now responsible for the design, development, and production for distribution in print and electronically on the Internet of all educational material approved by the Ministry of Education

- [ ] CTI is also responsible for developing educational policies with respect to the educational material for elementary and secondary school levels

New challenges

- CTI is now more actively involved in shaping current and future best practices in educational material

- CTI created during last year all electronic material that was recently distributed to students in the first two education levels

- CTI creates several distribution channels for the material approved by the Ministry of Education through the Greek School Network

The Greek School Network (GSN)

ABC4 TRUST

GSN is the **Educational Network** of MoE **– Eleven (11) years of operation**

It connects: **16.030** schools, **>8.000** school LANs, **899** education administration bureaus, lifelong learning organization, **594** libraries, **60** archives of the State, etc.

Provides personalized access to **77.382** teachers and **51.173** students.

Closed educational intranet – **security** for students is one of the prime objectives.

Develops, provides and supports **value added services**, specially designed for **education** and for **administration of education**.

Extended use of **open source** software.

Helpdesk: supports **>30.000 tickets/year** and a **multiple number** of phone calls

It provides the **«social» space** and the **means** for the creation of **Educational Networking Communities.**

Cofounded by **European Union** and **Greek state**

Designed, implemented and operated by the **Ministry of Education** and twelve Research Centers, Universities and TEI.

User categories

The **certification** of users is a **particularly powerful requirement**, because the character of the Network.

All users are certified with their identity through the central informational systems of the Ministry of Education.

User categories:

☐ Schools   **16.620**

☐ Administrative offices   **925**

☐ Teachers and staff   **77.382**

☐ Pupils   **51.173**

Communication Services
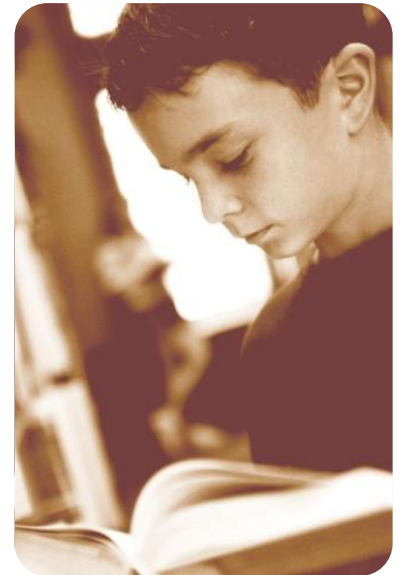
E-mail (webmail.sch.gr)

- ☐ Active inboxes: **135.000**
- ☐ Space: Teachers: **2.000 MB**, Students: **200 MB**
- ☐ 10 days **history**
- ☐ Virus and spam **protection**
- ☐ SMTP authentication
- ☐ Problem reporting and support
- ☐ Monthly use **> 35.000 users**
- ☐ Implementation using Postfix, Dovecot, Horde, Spamassasin, Clamav, etc
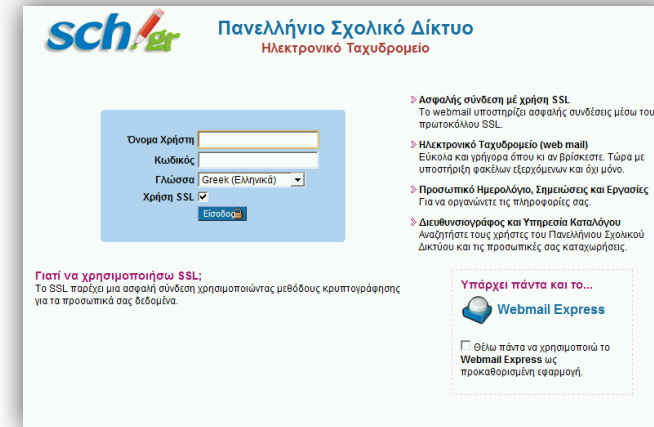
E-mail lists (www.sch.gr/lists)

- ☐ Official communication, distribution of circulars, documents, etc.
- ☐ Briefing of educational community
- ☐ Lists: central, prefectural, teachers, students, etc.
- ☐ Particularly popular service
- ☐ Implementation using Mailman, ezmlm

Web portals

School Portal (www.sch.gr)

- ☐ Entry in the electronic services
- ☐ Structured content for schools, teachers and students
- ☐ Educational catalogue: content in GSN services (eg. web pages and blogs)
- ☐ Announcements for educational events and news
- ☐ Live webcastings
- ☐ Discussion for and school magazines
- ☐ Technical support and statistics
- ☐ RSS Feeds and connections to social media (twitter, facebook, etc)
- ☐ Unique visitors **216.979** (May 2011)
- ☐ Implementation using Joomla

Online Communities

Online Educational Communities (blogs.sch.gr)

It is an educational designed Web 2.0 tool, that:

- ☐ Allows members to interact with each-other in a multi-blogging environment

- ☐ Provides the functionality of a modern social networking tool, such as: Groups, Friends, Private Messages, Advanced Member Profile, Aggregator of members and blogs activity, Wiki's, Forums, Member Status, RSS feeds, etc.

- ☐ All members are registered (teachers and students)

- ☐ Its design is based on pedagogical principles

- ☐ Is based on BuddyPress (an powerful extension of WordPress)

The school "Facebook" is here!
Educational and Safe !

What is the common element in all these services? User authentication!

- Most services are directed to registered users, who are involved in the educational system in Greece.

- In many cases, we also need to preserve user anonymity.

- On the other hand, beyond full anonymity, user societies and social groups (such as pupols or university students, for instance) are excellent targets for user profile directed opinion gathering and polls.

- How can anonymity coexist with user profile based services?

Current user authentication landscape

- Traditional cryptographic certificates (e.g. PKI based) are *bound* to the *identity* of a real person, which they fully disclose when provided.

- Showing these credentials implies a number privacy problems: (i) unnecessary disclosure of full identity (ii) user profiling (iii) impossibility of accessing in a *verifiable* yet *anonymous* way various services (e.g. medical databases or other specialized information repositories)

- However, many use cases require only knowledge of meta-properties of the user (e.g. user is over age 18 or a high school student) or of a subset of the user's identity elements.

Attribute Based Credentials (ABCs): privacy preserving authentication!

- ABC tokens cannot be combined and lead to the revelation of identity (***unlinkability property***)
  - Token issuance and token presentation are unlinkable
  - Think "coins" (cannot be distinguished) vs. "bills" (have a serial number!)

- Users can disclose a <u>subset</u> of the encoded user claims about his/her identity (***minimal disclosure property***)
  - To respond to unanticipated requests of RPs
  - Without invalidating the token integrity

ABC4Trust aims at Deploying Attribute-based credentials for privacy and trustworthy authorisation

1. Define a common unified architecture for ABC systems

2. Deliver open reference implementations with validation in actual pilots

ABC4Trust consortium

Johann Wolfgang Goethe-Universität Frankfurt, DE

Alexandra Institute AS, DK

Research Academic Computer Technology Institute, GR

IBM Research - Zurich, CH

Miracle A/S, DK

Nokia-Siemens Networks GmbH & Co. KG, DE

Technische Universität Darmstadt, DE

Unabhängiges Landeszentrum für Datenschutz, DE

Eurodocs AB, SE

CryptoExperts SAS, FR

Microsoft Research And Development France, FR

Söderhamn Kommun, SE

Yannis Stamatiou, CTI

The Greek Pilot in a nutshell: Course Evaluation by Certified Students

- Informal course evaluations conducted anonymously without lecturers knowing participant's identities

- Based on student attendance information

- Issuance of multiple credentials (student ID info, course registration info, class attendance info)

- Verification with *anonymous proofs* towards "untrusted" infrastructure

- A precursor for the introduction of ABC4Trust innovations in the Greek School Network and all the Greek Educational Community

CEID and CTI

- Co-located in the University of Patras campus

- Close collaboration (many faculty members of CEID collaborate with CTI and vice versa)

- Established in 1985

- 5-year computer engineering curriculum

- Accepts ~250 new students each year

CEID

CTI

- Established in 1985

- Undertakes R&D ICT projects

- It has 10 distinct activity sectors

- Employs about 200 employees with ~40 MSc or PhD holders

✓ Two courses have been selected to be evaluated from the 5 year (10 semester) curriculum of the Computer Engineering and Informatics Department (CEID), at the University of Patras, Greece.

✓ Distributed Systems I (A 7th semester theoretical class which has already started):

 ✓ Number of attending students: approximately 80.

✓ Operating Systems (A 6th semester laboratory Class):

 ✓ Estimated number of students: 200.

High Level Architecture / Patras Pilot
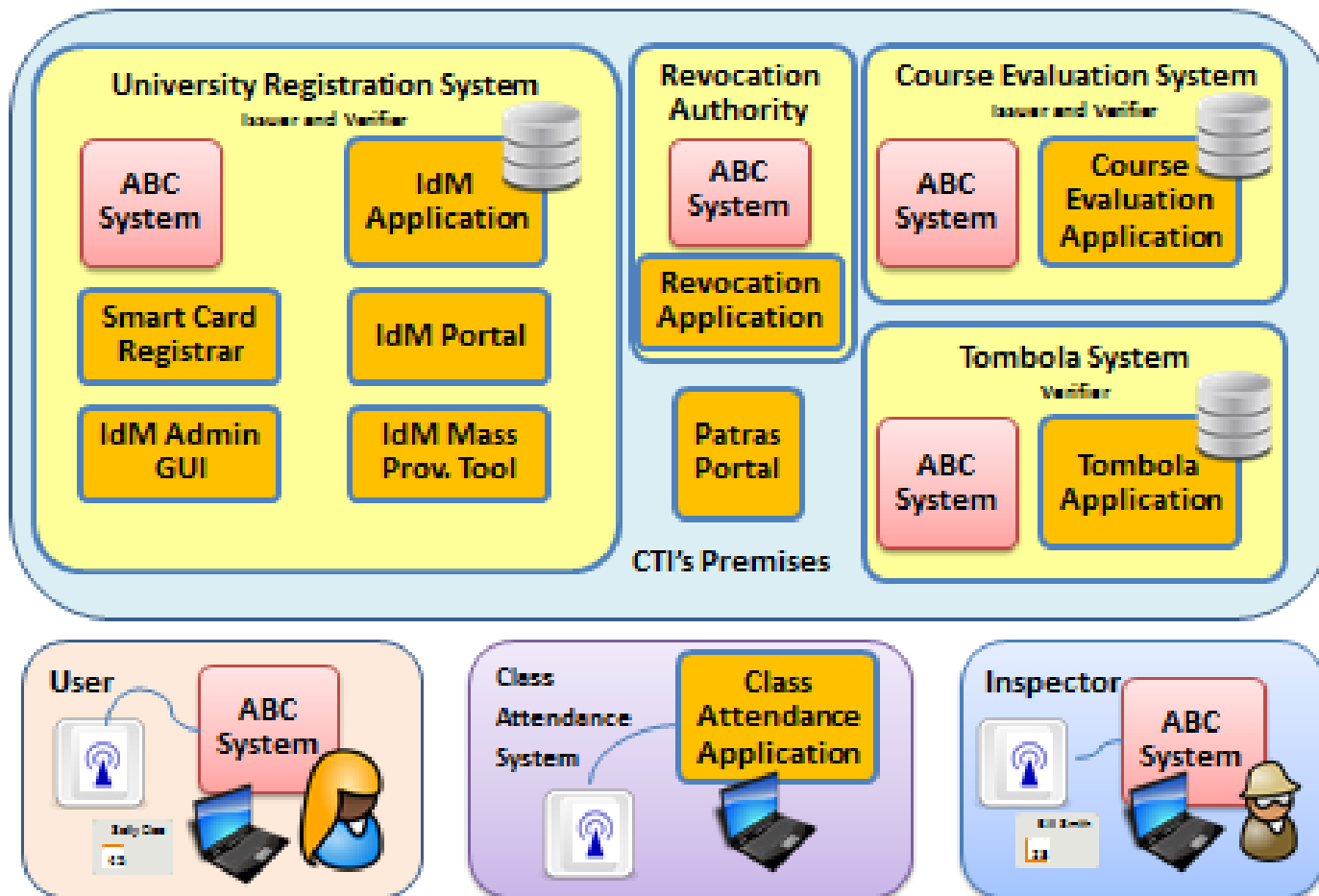
Student Credentials for the second round

1. **University Credential**

   (Idemix)

2. **Course Credential**

   (U-Prove)

3. **Tombola Credential**

   (Idemix)

credUniv (revocable):

- First Name:
- Last Name:
- University Name:
- Department Name:
- **Matriculation Number:**

credCourse:

- Course Identifier:

credTombola:

- **Matriculation Number:**

Carry-over attribute:

Participating in the Pilot

Beginning of the Semester

- Get Smart Card
- Register Smart Card
- Get a University Credential
- Get a Course Registration Credential

During the Semester

- Collect Class Attendance Evidence
- Periodic Backup of Smart Card
- Smart Card Restore in Case Needed

In the end of the Semester

- Participate in the Course Evaluation
- Obtain Tombola Credential (if so desired)
- Participate in the draw to win a prize
- Inspect the Tombola Credential to identify the winner
- Revoke the University Credential, if necessary

University Pilot Portal

From the University Pilot Portal students can access the following:

- ✓ The University Registration Server in order to collect their credentials.

- ✓ The Course Evaluation Server in order to evaluate the target course.

- ✓ The required software for interacting with the systems.

- ✓ Instructions manual.

The entry to the pilot: The University Pilot Portal

- The University Pilot Portal is a web information and system access portal for the pilot (https://ces.cti.gr/Portal/Portal.html)

Yannis Stamatiou, CTI
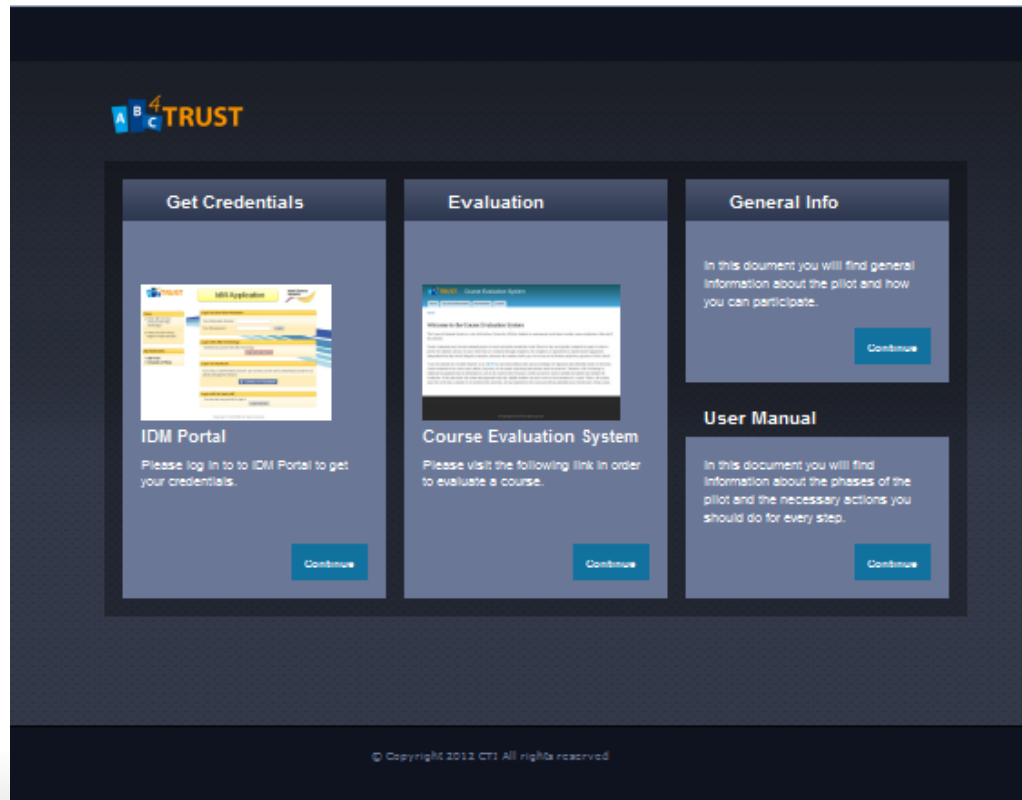
Student's equipment

☑A smart card.

☑A smart card reader.

☑A sealed envelope that is marked with the smart card ID and contains the smart card's PIN and PUK.

☑A slip of paper containing a one-time-password (OTP) for accessing the University Registration System.

Zooming in:
Collecting Course Attendance Units

- ✓ Students are issued course credentials on smart cards before each semester begins.

- ✓ Students entering the course lecture room wave their smart card in front of a contactless reader – we use a contactless reader to avoid long queues of students waiting to insert their cards in a contact readers.

- ✓ The students access (in the end of the semester) the course evaluation system and are allowed to evaluate the course, if they are eligible.

Yannis Stamatiou, CTI

Collecting Course Attendance Units
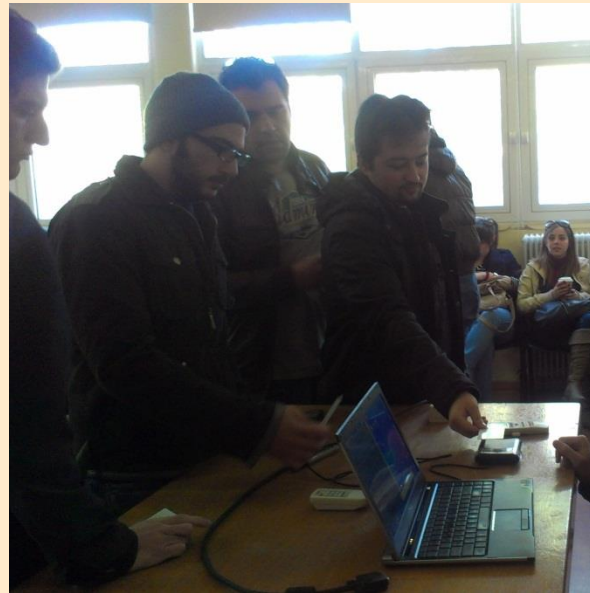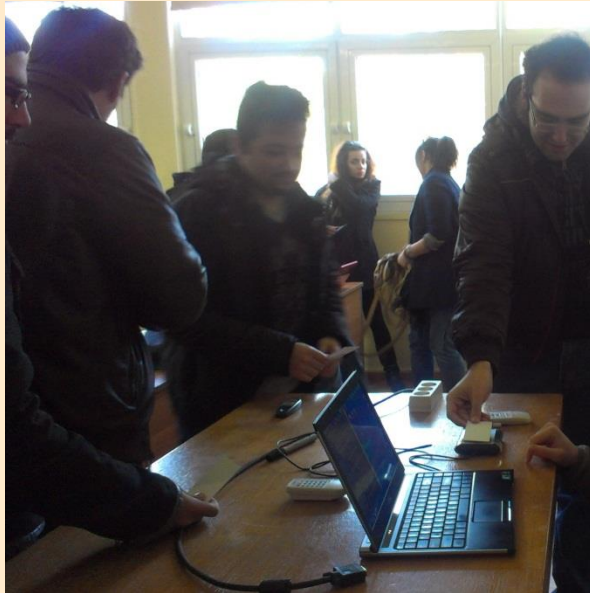
✓ Students Collecting Attendance Units

✓ The Lecture Room

✓ The Class Attendance System

✓ A student accesses the course evaluation system through the portal.

✓ Using the credentials stored on the smart card the student can participate in the course evaluation after proving that they:

  ✓ have registered the university course under evaluation (i.e. they have CredCourse).

  ✓ have attended the minimum required number of course lectures (if this minimum is set to 0, all students are allowed to participate).

We will demonstrate the following use cases:

- Obtaining credentials from the *University Registration System*
- Obtaining attendance units using the *Class Attendance System*
- Participating in the course evaluation using the *Course Evaluation System*
- Carry-over attribute

  (matriculation number from University credential to Tombola credential)
- Inspection for identifying the Tombola winner, using the *Inspection feature*
- Revocation of the University credential using the *Revocation System*

Yannis Stamatiou, CTI

Demo steps

Steps of 1st round:

First time login using OTP

Registering smartcard

Obtain University Credential

Obtain Course Credential

List credential attributes

Login with smartcard using Privacy-ABCS

Collecting attendance unit #1

Attempt to evaluate course
• To be rejected (attendance threshold is 2)

Collecting attendance unit #2

Attempt to evaluate course
• To be successful

Additional steps of 2nd round:

Obtain Tombola credential using the matriculation number as a carry-over attibute

Registration to the Tombola system for the lottery draw

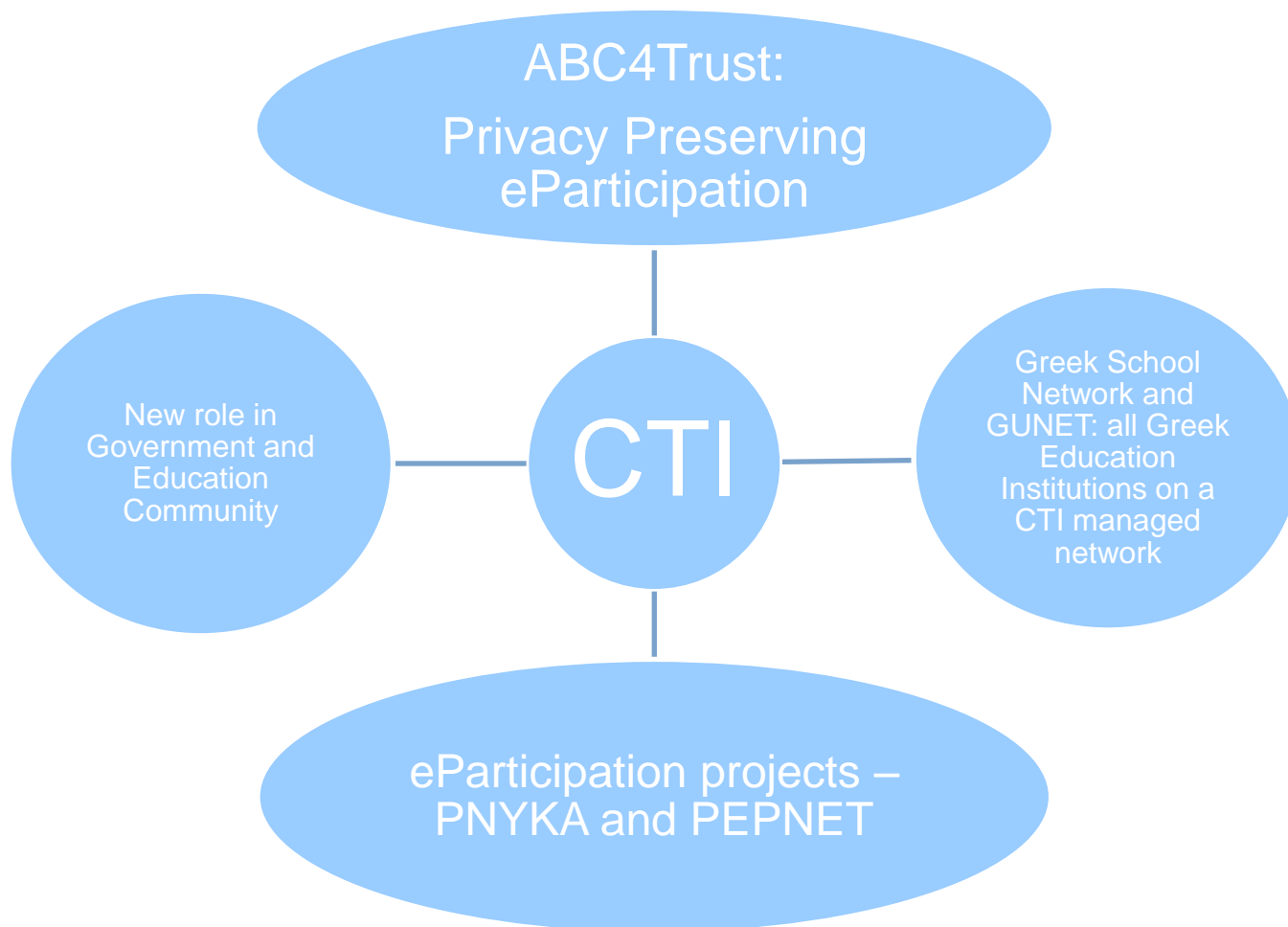Lottery draw and identification of the winner using Inspection

Login to the Revocation server using administrator's smart card

Revocation of the University Credential
• List credentials to see revoked University credential
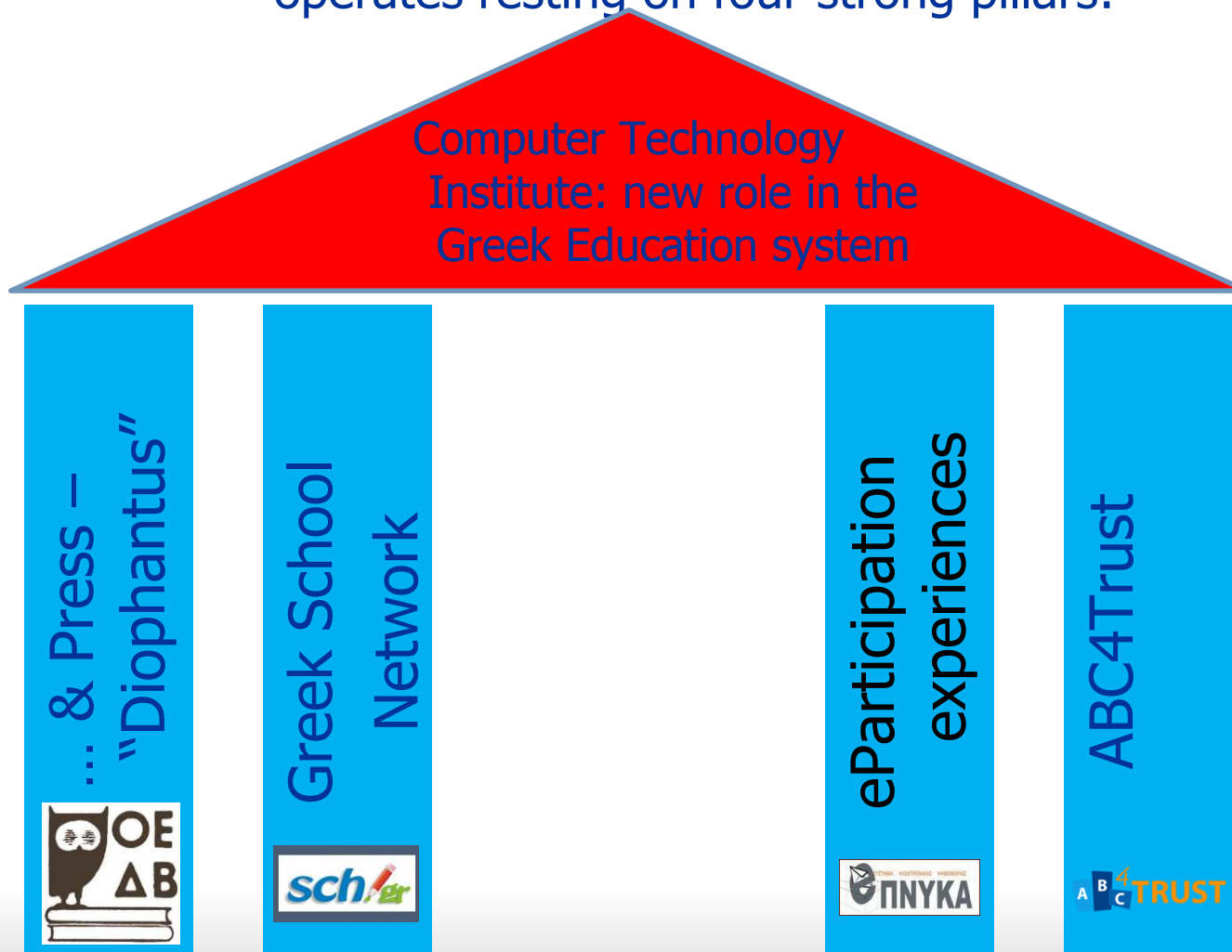
In summary …

ABC4Trust:

Privacy Preserving eParticipation

New role in Government and Education Community

CTI

Greek School Network and GUNET: all Greek Education Institutions on a CTI managed network

eParticipation projects – PNYKA and PEPNET

Thank you!

www.abc4trust.eu

Questions?

ABC4TRUST

SEVENTH FRAMEWORK
PROGRAMME