

# AAI Model and Standard in CSTCloud

*LI Jianhui*

Computer Network Information Center, CAS

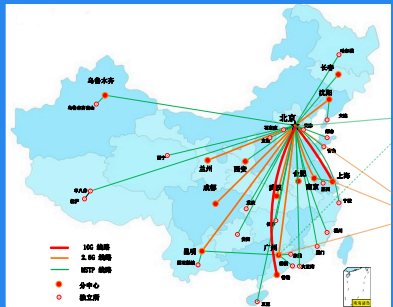
@Technical Discussion on AAI model for GOSC framework 31st March 2022

# CSTCloud Overview

- CSTCloud is included in the 13th Five-Year Plan for National Informatization as one of the **key national e-infrastructures**.
- CSTCloud fully supports multidisciplinary open scientific research with integrated cloud services for the **discovery, usage, and delivery of S&T resources**.



Pool of research software



High-speed network connection



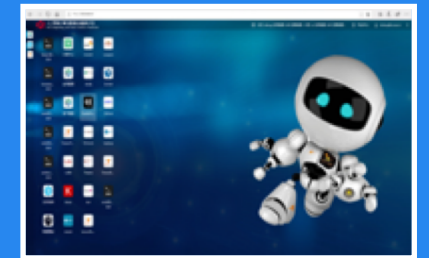
Computing resources



Data & Information



Algorithms & tools

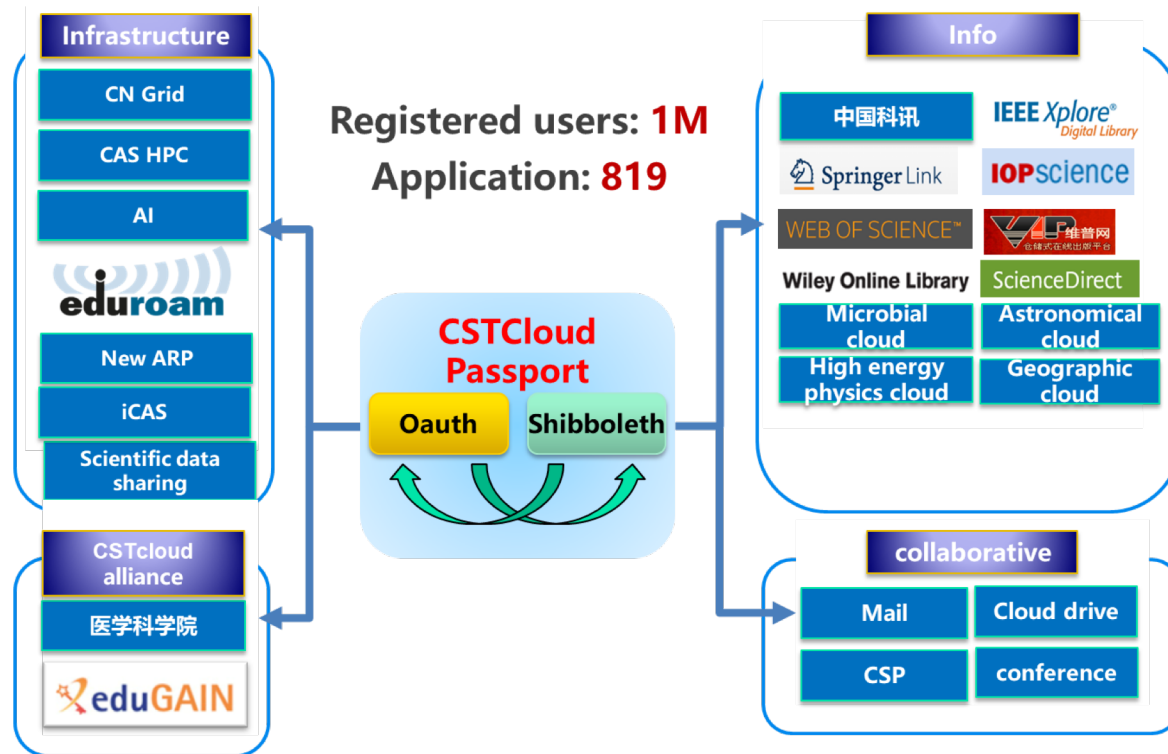


Massive data storage



# CSTCloud ID - Overview

- A **centralized, single sign-on** identity authentication and authorization system.
- An ID system that facilitates CAS researchers to access research resources and services across CAS and around the nation.



Apr. 2013 inaugurated

>1 M registered users

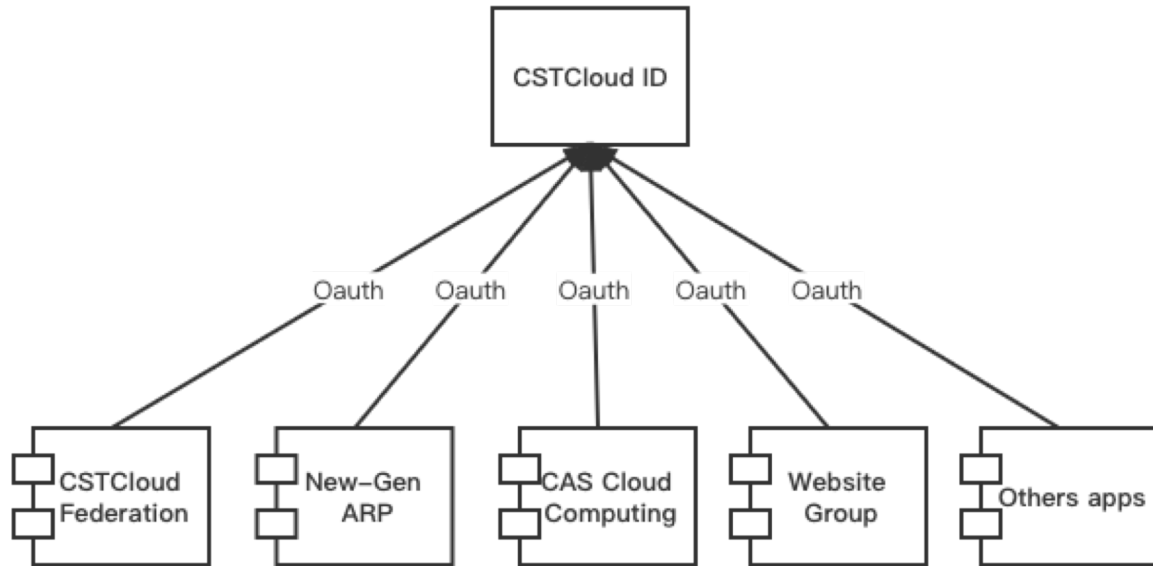
>95% CAS Institutions

≈ 270,000 visits per day

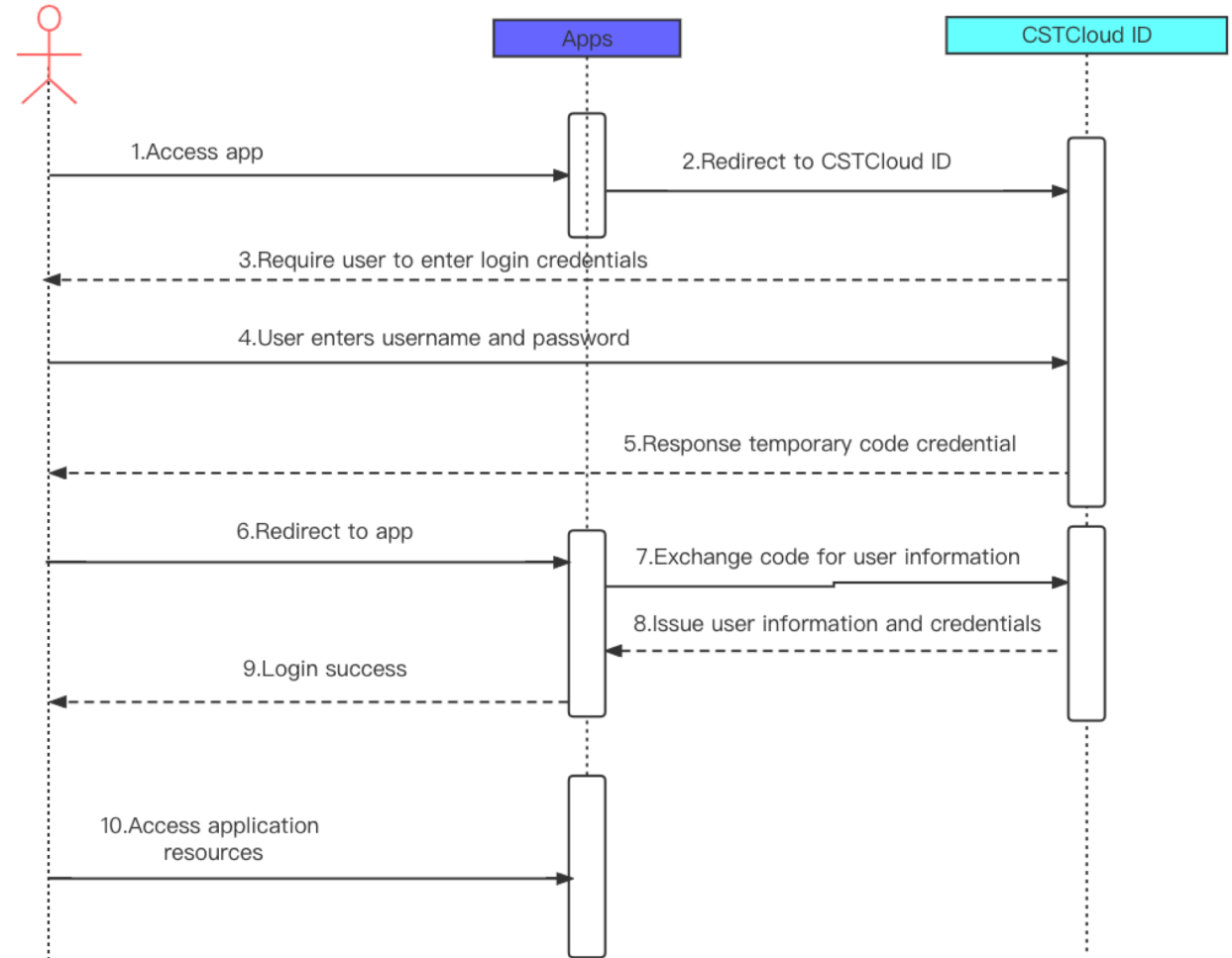
>800 applications (OAuth 2.0)

# Structure and Workflow

## Structure



## Workflow





# Application and Security Strategy

## Three Types of SPs

- CAS genetic SPs
- CAS institutional-level SPs
- Open Science SPs

## User Security Policy

- Self-registration with verified E-mail accounts and phone numbers.
- Institute administrators control E-mail accounts.
- Strong password strategies.
- Dual verification for login.

### Mobile security certification

Your login device has changed, please enter the correct SMS verification code and

Security Phone

[Get verification code](#)

Phone Verification Code

[Save](#)

[2516](#)

### Sign Up CSTCloud passport

\* True Name

\* Image Text  [Change it](#)

\* CSTCloud ID

[Get verification code](#)

\* Mail Verification Code

\* Phone Number

[Get verification code](#)

Phone Verification Code

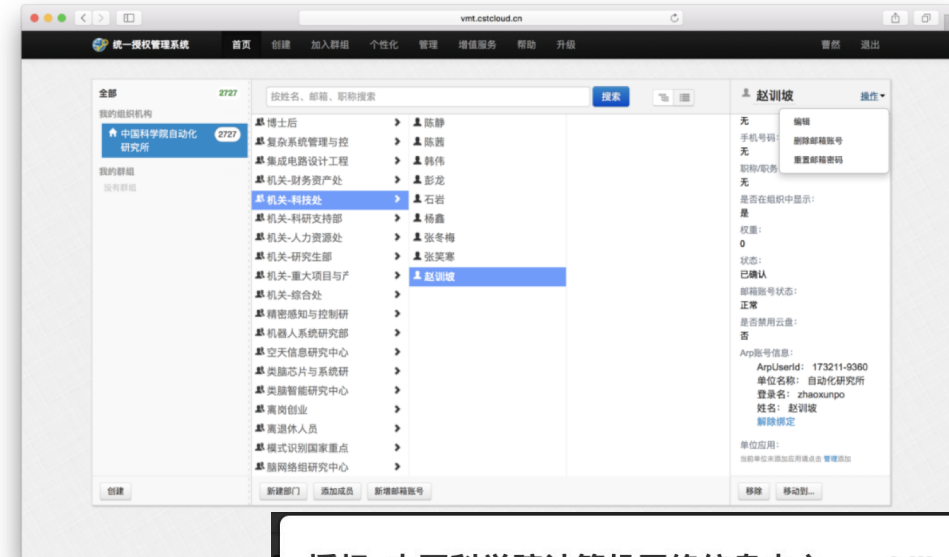
ID Card Number

Orgnization

\* Password

# Unified Authorization via VO

- One VO per institute, with a total of 179 VOs.
- Each VO is associated with multiple OAuth applications.
- VOs provide authorization services to allow users access to particular applications.



授权: 中国科学院计算机网络信息中心-xuzhijian@cstnet.cn

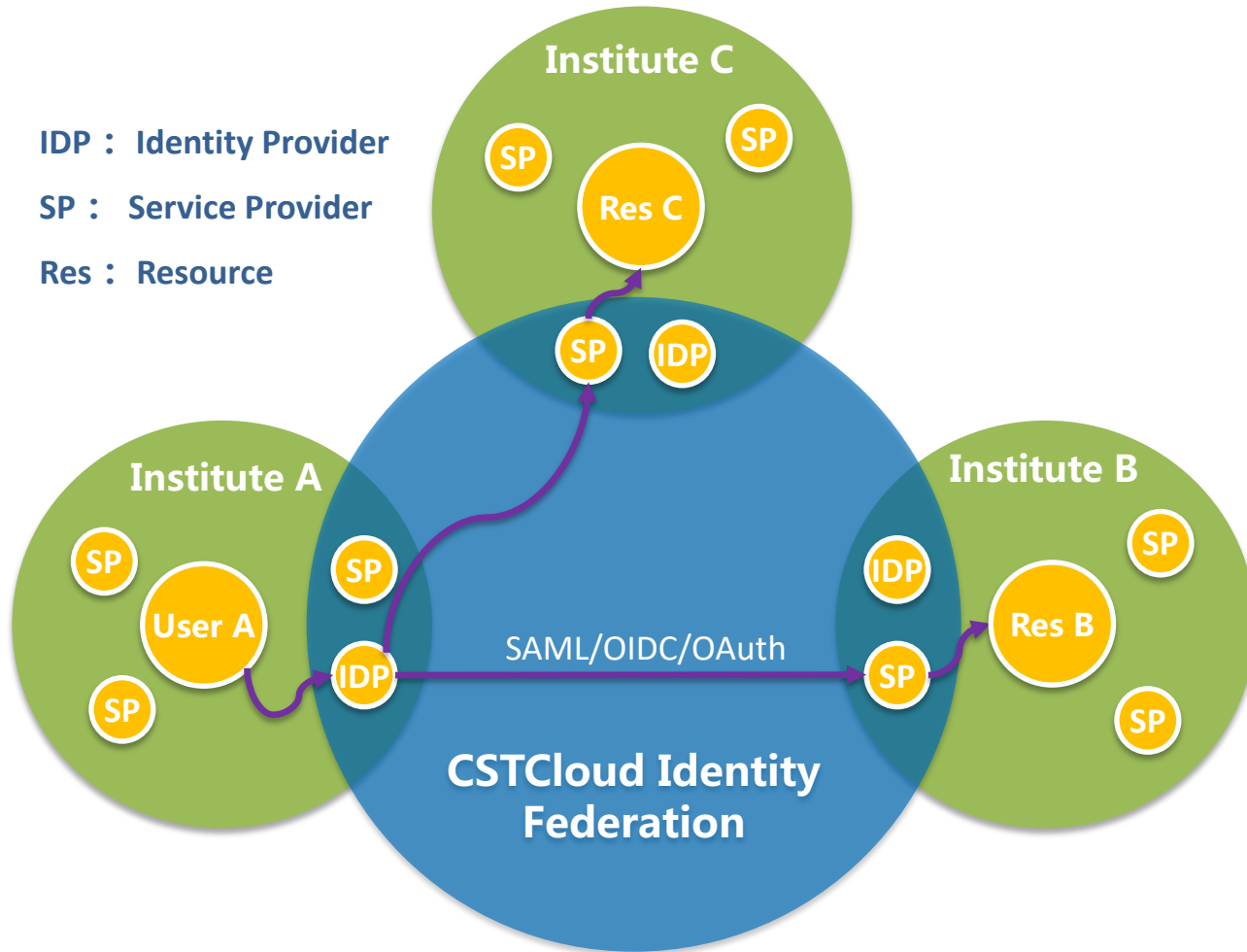
授权访问或取消授权会将该单位或部门下面所有用户给予或取消访问应用的权限

- 新一代ARP系统 (已授权)
- 新一代ARP系统VPN (已授权)
- 新一代ARP国际合作 (已授权)

[授权访问](#) [取消授权](#)

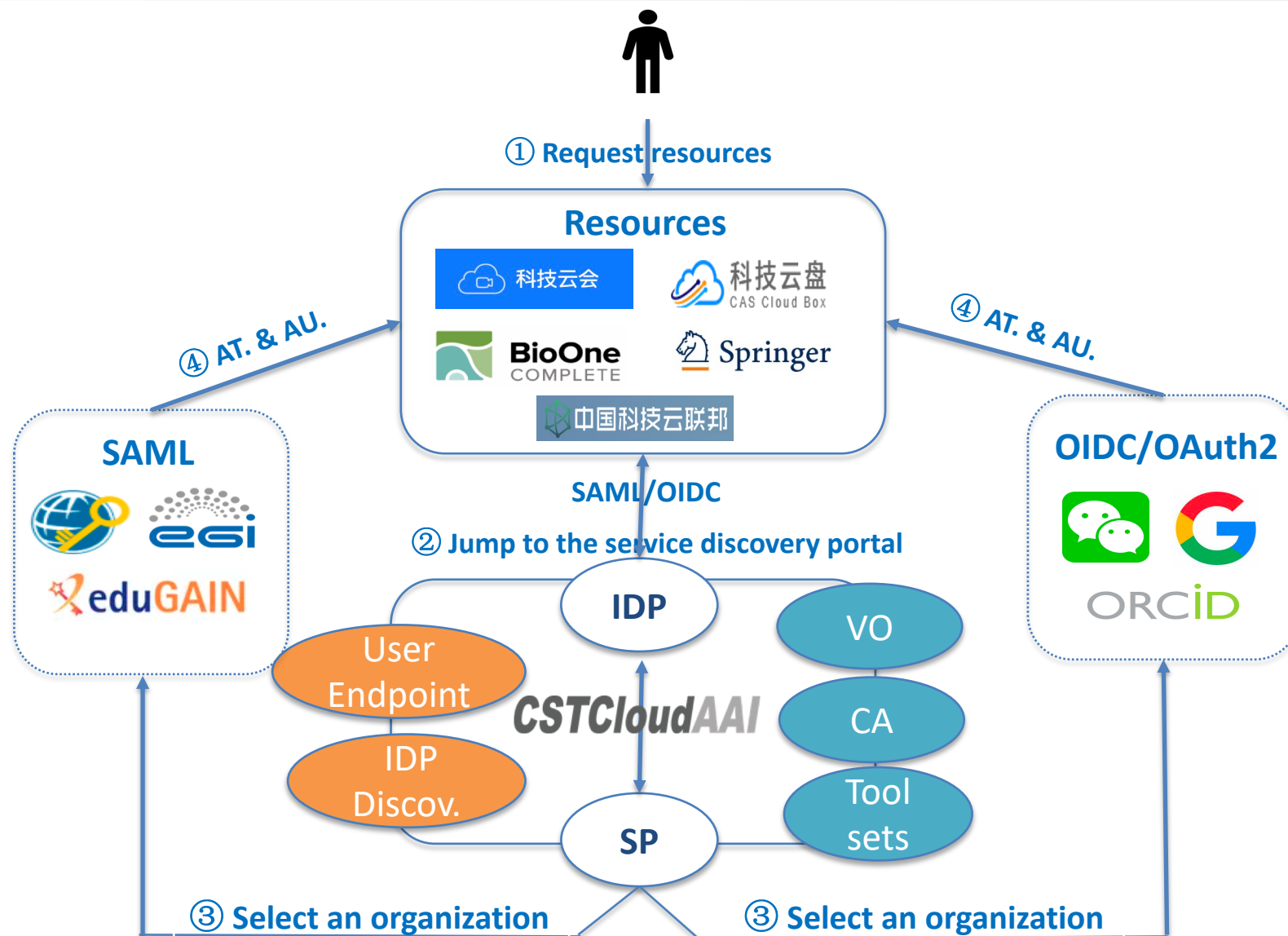
- The **increasing number of external accounts** is challenging and costly to manage, with relatively lower user acceptance.
- Large-scale application systems/resource platforms prefer to build their own user account system with **third-party login**.
- There is no **international academic cooperation standard** applicable to CSTCloud ID.

# Embracing CSTCloud AAI



- Re-design and develop a sustained and robust system with federal user identity authentication and authorization that can enable access to open and convergent global resources.
- Facilitate interoperability of cloud resources services under fair conditions.

# CSTCloud AAI - Workflow for Tailored Scenarios



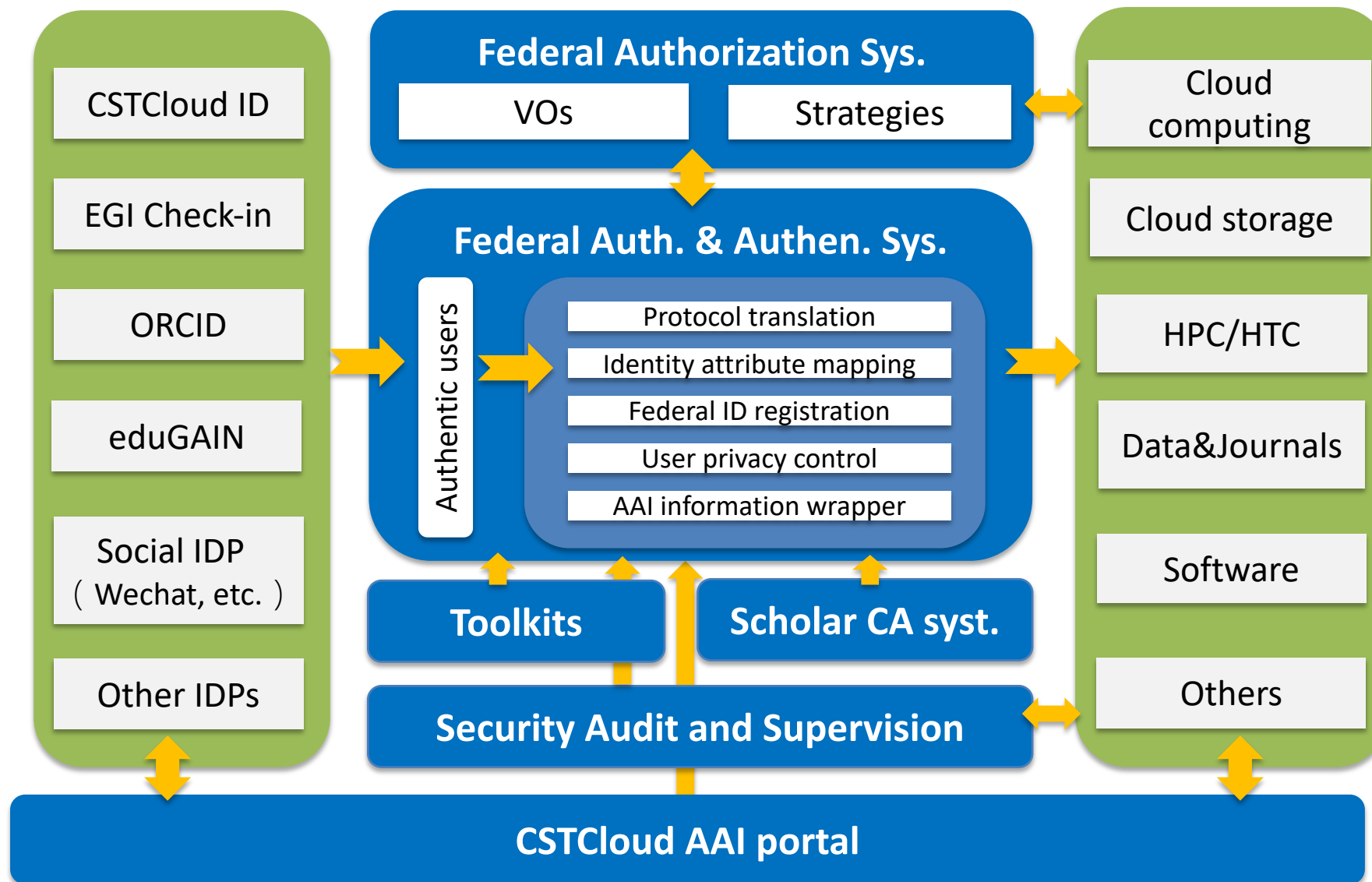
## Roles:

- Federation IDP
- Federation SP
- Virtual Organization (VO)
- User

## AAI Services:

- IDP Discovery Service
- CA Certificate Service
- Software toolsets

# CSTCloud AAI - Technical Framework



# CSTCloud AAI - Progress

Apr. 2020

EGI check-in system connects CSTCloud AAI as IDP.

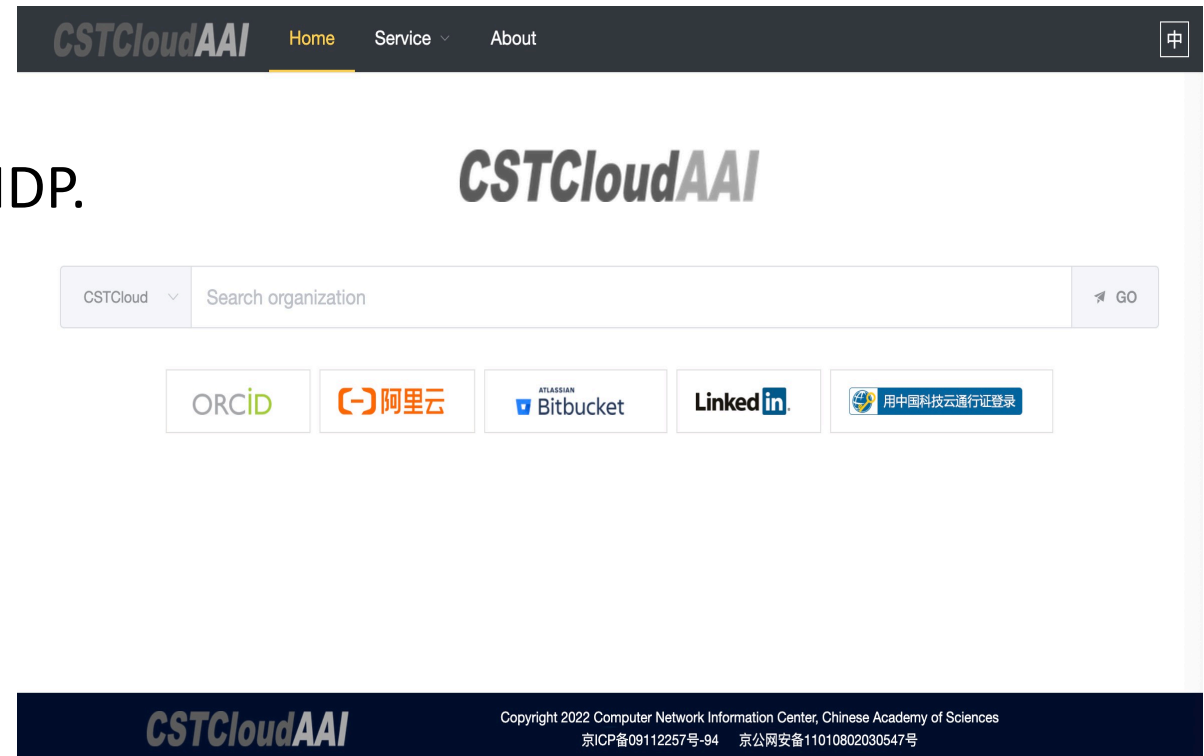
Sep. 2020

CSTCloud AAI becomes a member of eduGAIN.

Dec. 2021

Inaugurated prototype system online.

- ✓ Integrated with all eduGAIN IDPs.
- ✓ Support protocols (i.e. SAML/OIDC, IDP/SP).
- ✓ Integrate some social apps/cloud services IDPs.



<https://aai.cstcloud.net>



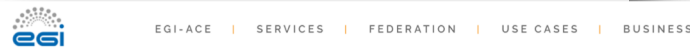
# CSTCloud AAI - International Alignment

CSTCloud facilitates interconnection by joining eduGAIN

Date: Oct 15, 2020

China Science and Technology Cloud (CSTCloud), initiated by the Chinese Academy of Sciences (CAS) and implemented by the academy's Computer Network Information Center (CNIC), joined the global identity federation community eduGAIN in early October. eduGAIN is a global community which connects 69 identity federations with more than 2800 identity providers and 5000 service providers. Becoming a member of eduGAIN will help facilitate cross-border flow of digital resources contributed by the Chinese research community and guarantee the consolidated foundation for the connectivity between CSTCloud and other research e-infrastructure:

CSTCloud is a national platform to provide scientists with other aspects of sharing scientific information and relevant scientific data centers and more than 80% national research disciplinary boundaries and key international research projects, such as the Five-hundred-meter Aperture Spherical Telescope observations with the Five-hundred-meter Aperture Spherical Telescope (FAST) and the Large-High-Altitude Air Shower Observatory (LHAASO). CSTCloud provides secure and open access by working with global federated Open Science Cloud (GOSC), which has been supported by continental open science cloud demonstration test-bed. CSTCloud will ensure interoperability with e-infrastructures out of China to support



## A federation of cloud resources beyond Europe

Julia Popescu | 14.09.2021 | EGI-ACE news, News | Share

Integration of China's CSTCloud with the EGI Federation has been recently completed. CSTCloud is a certified provider of the federation and meets all the operational tests for production usage.

Operated by the Computer Network Information Center (CNIC) of Chinese Academy of Sciences (CAS), CSTCloud is a national infrastructure for CAS scientific communities and China's top research. The design of the CSTCloud is based on the principle of 'openness and sharing'. It aims to develop an open architecture that is capable of integrating various national and international computing resources in order to support multidisciplinary open science research. CSTCloud provides computing facilities for Chinese advanced research projects including CASEarth, CAS Space Science Missions, and research related with big facilities or observation stations such as the Five-hundred-meter Aperture Spherical Telescope (FAST) and the Large-High-Altitude Air Shower Observatory (LHAASO).

The integration work is delivered under the EGI-ACE international cloud integration task force. There have been many challenges — different technical environments, different development culture, limited documentation, no previous examples, etc.

It has taken a number of months of effort and people from different organisations and teams are involved. Particularly, we are grateful to Professor Jianhui Li's team in CNIC, including the CNIC Cloud team (Haiming Zhang, Zuliang Guo, and Xiangguang Zheng), the CNIC AAI team (Yihua Zheng and Taotao Shi), and the CNIC Project Management team (Lili Zhang). Thanks to the EGI teams who provide dedicated supports, including the

- Potential Alignment with the Global Open Science Cloud Initiative CS

Incoherent scatter radar data

SDG-13 climate change and natural disasters

- Welcome for more collaboration!

In this case, the EISCAT and SYISR radar data fusion and computing may require further technical supports from the GOSC Initiative within the following aspects:

1. Secure check-in services for accessing cross-border cloud services
2. DIRAC for job submission
3. Radar data: 1. Secure check-in data services for accessing cross-border services for improving modelling, simulation, and
4. On-demand prediction.
  2. Data sharing model(s) and federated data activities.
  3. Collaborations on necessary activities for community engagement, involving CASEarth4SDGs and other initiatives, and with a focus on SDG-13.

**CSTCloudAAI**

 **eduGAIN**



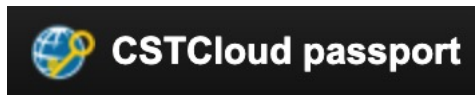
# CSTCloud AAI – Deployment

## IDPs (20+)

- International organizations
- CAS institutes
- Universities
- Others

## SPs

- CAS Conference Service Platform
- SDG Workbench
- Code Repository for SDG Workbench
- Jupyterhub for SDG Workbench
- Jupyterhub for Radar data on GOSC Testbed



中国科学技术大学



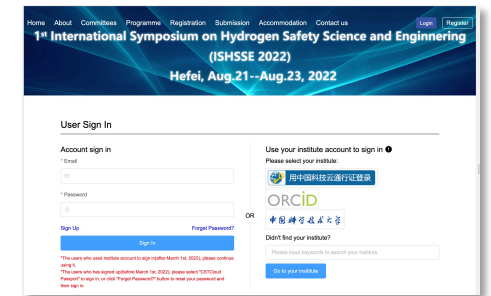
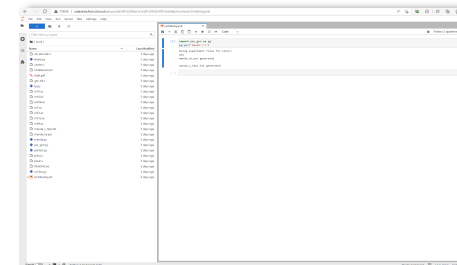
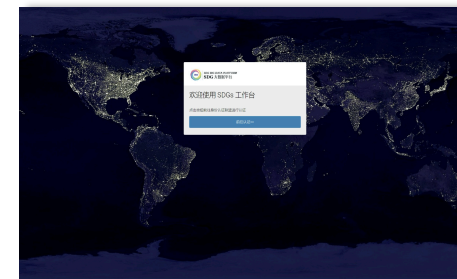
香港中文大學(深圳)  
The Chinese University of Hong Kong, Shenzhen



湖南大學  
HUNAN UNIVERSITY



澳門大學  
UNIVERSIDADE DE MACAU  
UNIVERSITY OF MACAU



# The next step

## Enhanced authorization management based on VO

- To facilitate the operation flows with enhanced management functions.
- To support the integration of applications.

## Certificate management and X.509 authentication

- To support authentication in accessing applications.
- To facilitate CSTCloud AAI users apply for their own certificates.

## Security, Audit, and Monitoring

- To protect user behaviors and data security.

## International engagement

- To refine policy for open science.
- To facilitate research resources flow based on the GOSC testbed.

# Connection with EGI

- Access CSTCloud AAI with EGI AAI check-in account.

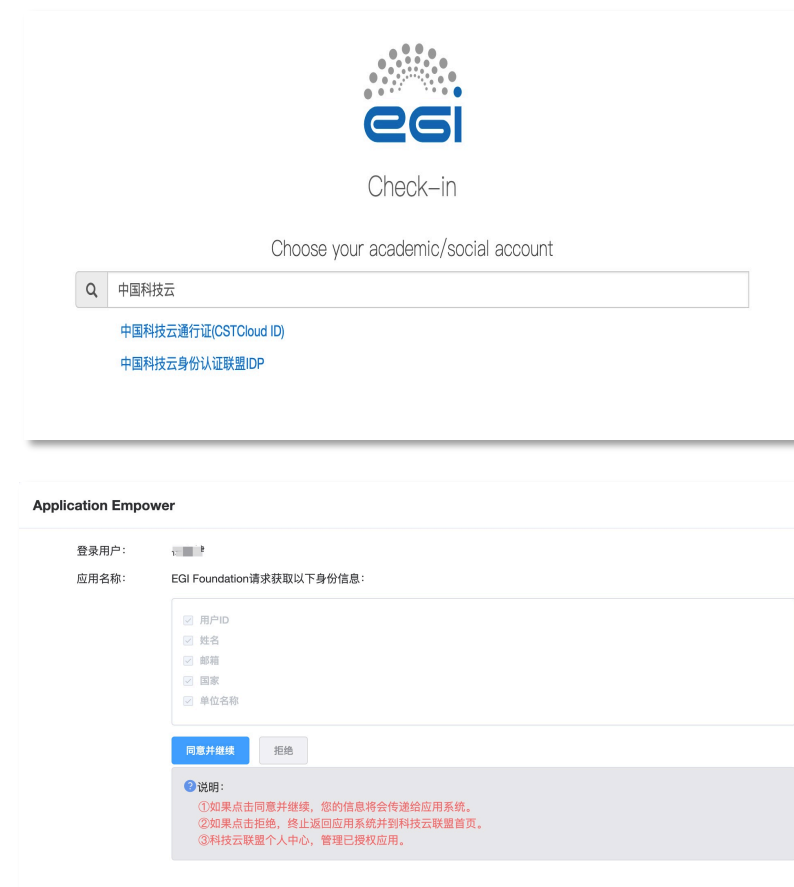


The screenshot shows the EGI Check-in interface. At the top is the EGI logo and the text "Check-in". Below this, it says "CSTCloud AAI请求以下信息被传送。" (CSTCloud AAI requests the following information to be transmitted). There are four input fields with labels and values:

邮箱	member@cstnet.cn
家庭联络地址	member@cnic.ac.cn
名	成员
显示名称	成员

At the bottom, there is a "Community User Identifier (eduPersonUniqueId)" field with the value "c1910b0e6c7b0230deef1bea13e515ac4f312e7f386409a62b7055fc543a526@egi.eu".

- Access EGI AAI with CSTCloud AAI check-in account.



The screenshot shows the EGI Check-in interface for EGI AAI. At the top is the EGI logo and the text "Check-in". Below this, it says "Choose your academic/social account". There is a search bar with the text "中国科技云" (CSTCloud) and two search results:

- 中国科技云通行证(CSTCloud ID)
- 中国科技云身份认证联盟IDP

Below the search results is the "Application Empower" section. It shows the "登录用户" (Login User) field and the "应用名称" (Application Name) field with the value "EGI Foundation请求获取以下身份信息:" (EGI Foundation requests the following identity information:). There are four checkboxes for the information to be transmitted:

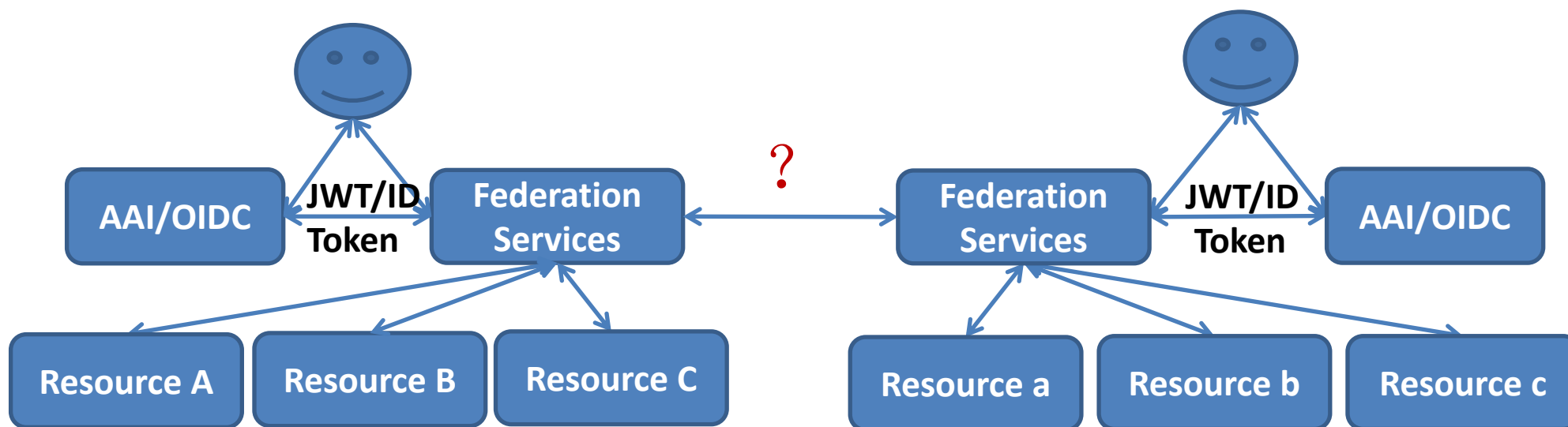
- 用户ID
- 姓名
- 邮箱
- 国家
- 单位名称

At the bottom, there are two buttons: "同意并继续" (Agree and Continue) and "拒绝" (Reject). Below the buttons is a "说明" (Note) section with three points:

- ①如果点击同意并继续, 您的信息将会传递给应用系统。
- ②如果点击拒绝, 终止返回应用系统并到科技云联盟首页。
- ③科技云联盟个人中心, 管理已授权应用。

# Discussion

- Exploring protocols that can be used for peer-to-peer resource exchange across cloud federations, while reserving control rights for local resources.



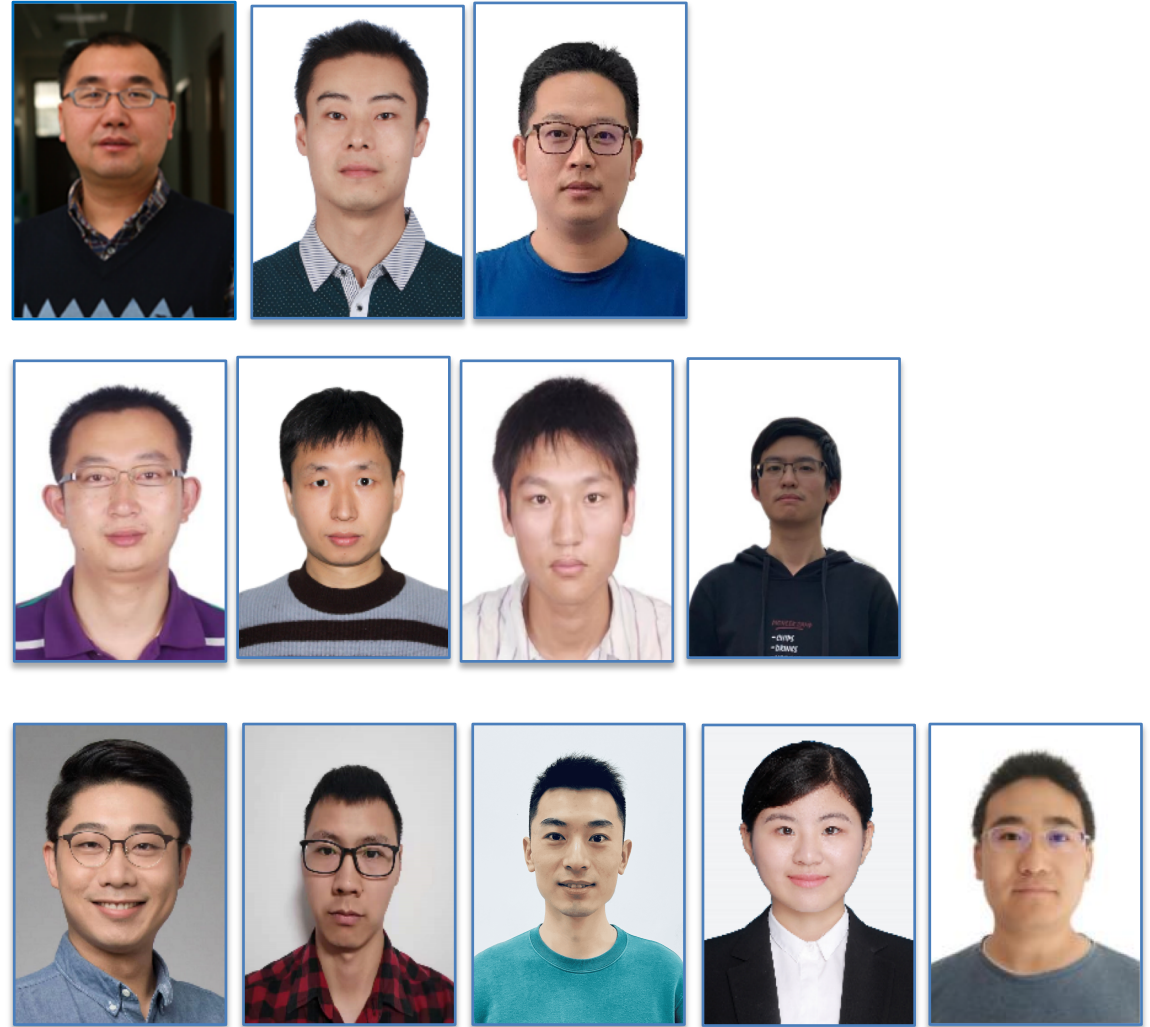
# Acknowledgement

- This work is supported by the Chinese Academy of Sciences (241711KYSB2020002), Ministry of Science and Technology, P.R.C. (2021YFE0111500) and Beijing Municipal Science & Technology Commission, China (Z201100008320027)

**CSTCloudAAI**

 中国科技云联邦

 用中国科技云通行证登录





Thank you!

*LI Jianhui*

Computer Network Information Center, CAS

@Technical Discussion on AAI model for GOSC framework 31st March 2022



中国科学院  
计算机网络信息中心  
Computer Network Information Center,  
Chinese Academy of Sciences