

# Single Sign On and Authorization Infrastructure using CAS<sup>2</sup>

**Shoji KAJITA (Information Technology Center, Nagoya University)**

**and**

**Hisashi NAITO (Graduate School of Mathematics, Nagoya University)**

# Plan of Talk

---

- Short introduction for CAS and CAS<sup>2</sup>
- Authentication mechanism of CAS and Authorization mechanism of CAS<sup>2</sup>
- “Nagoya University Portal” using CAS<sup>2</sup>
- Summary

# What is CAS & CAS2

---

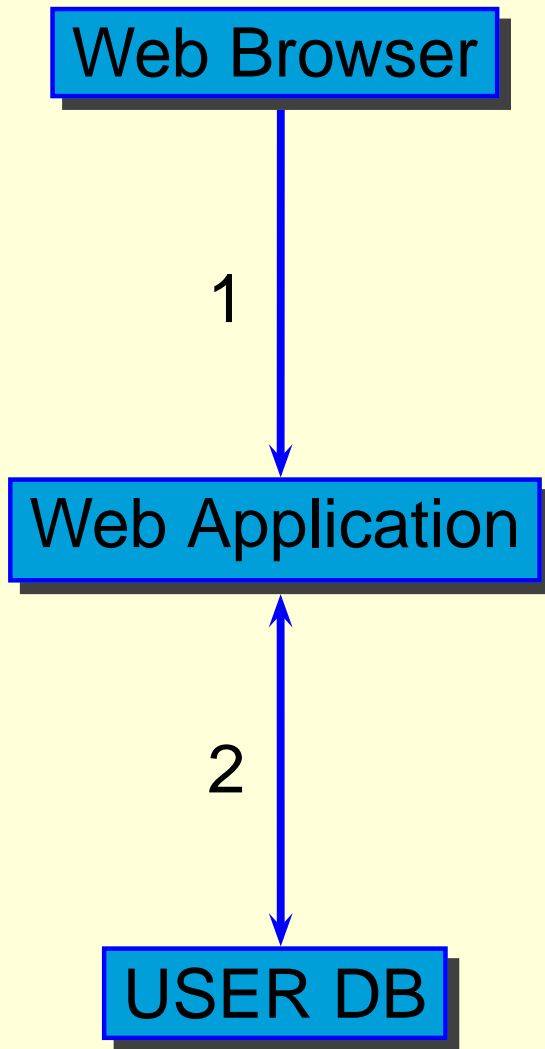
## ● CAS

- Single Sign On Environment for [Web Applications](#)
- Open Source software developed by Yale University

## ● CAS<sup>2</sup>

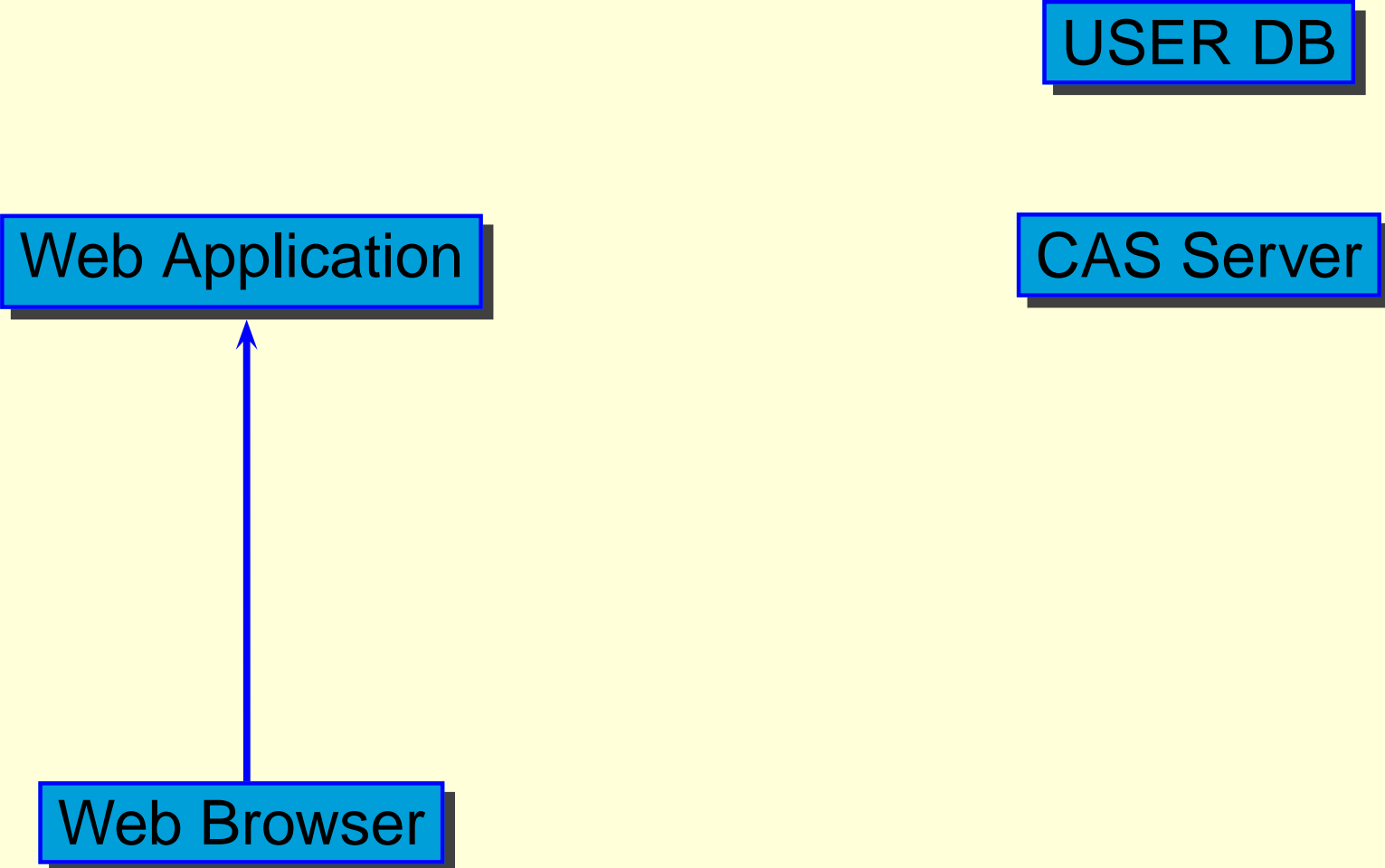
- We extends to [Authorization](#) Environment for [Web Applications](#)
- CAS<sup>2</sup> controls Access Rights for each Web Application
  - [WHO](#)
  - [WHEN](#)
  - [from WHERE](#)

# Usual Authentication and Authorization

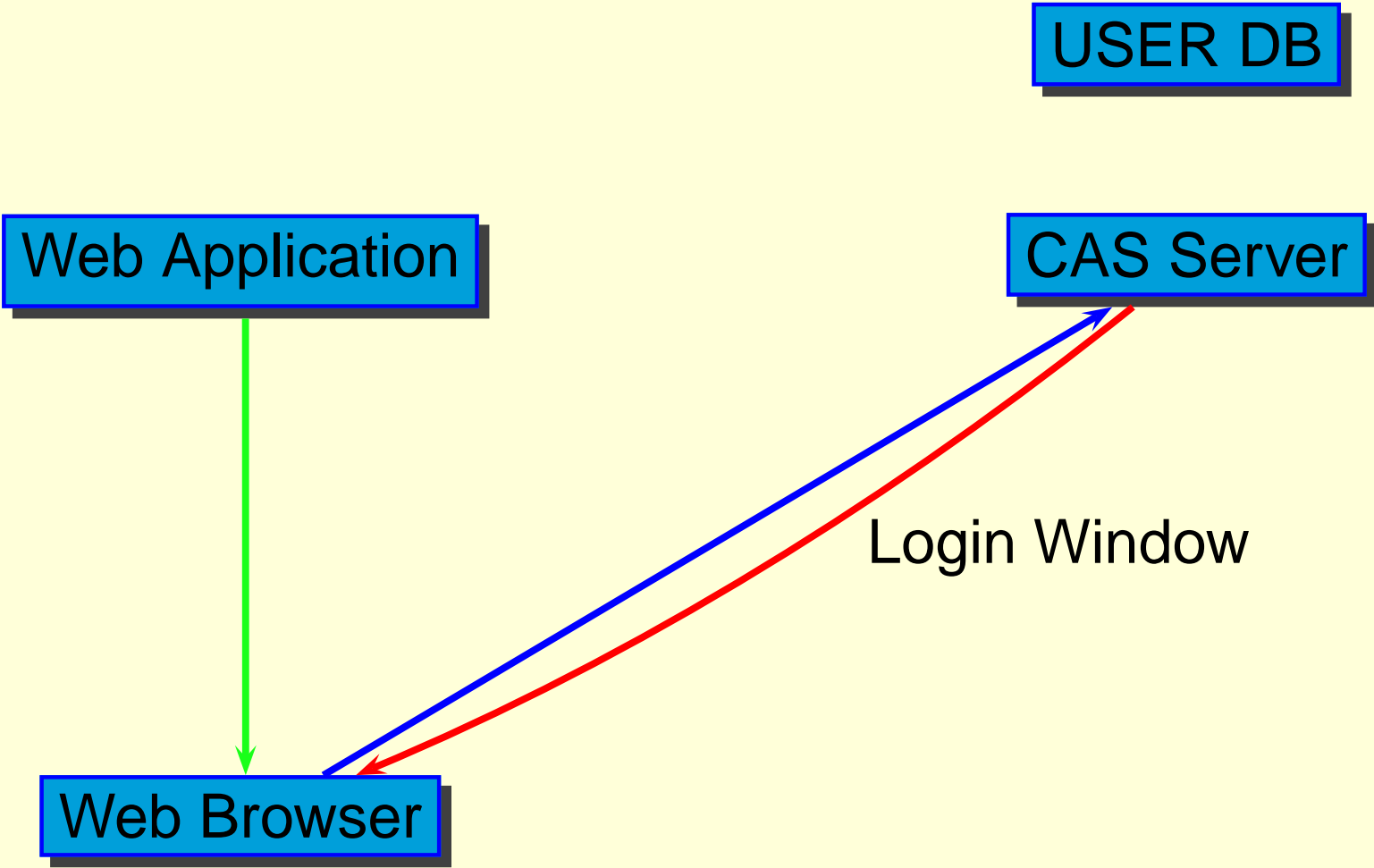


- Web Application must include AuthN & AuthZ codes
- Web Application **directly** accesses to USER DB to obtain User Information
  - Web Application has a **password** to access to USER DB

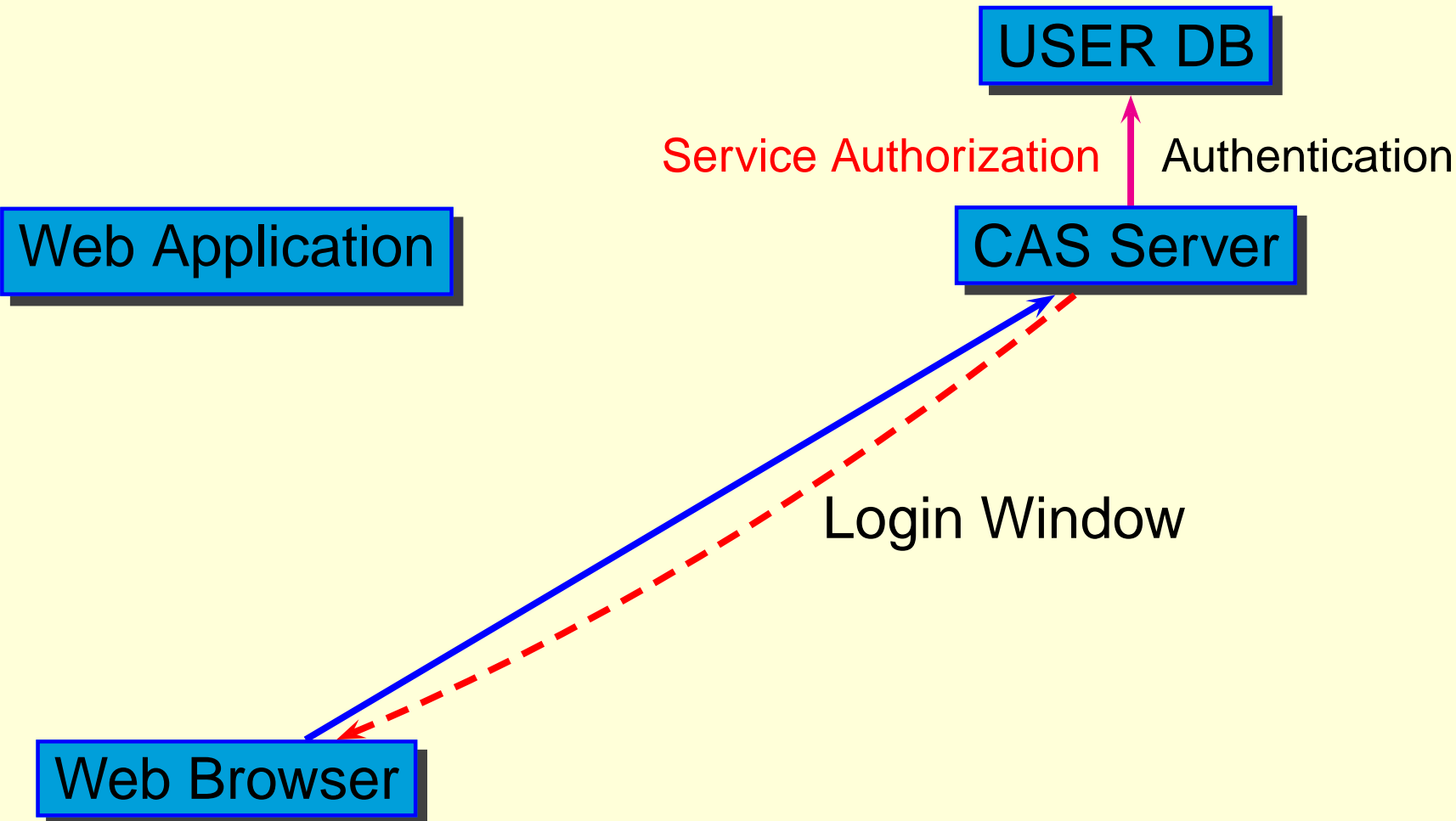
# Mechanism CAS and CAS2



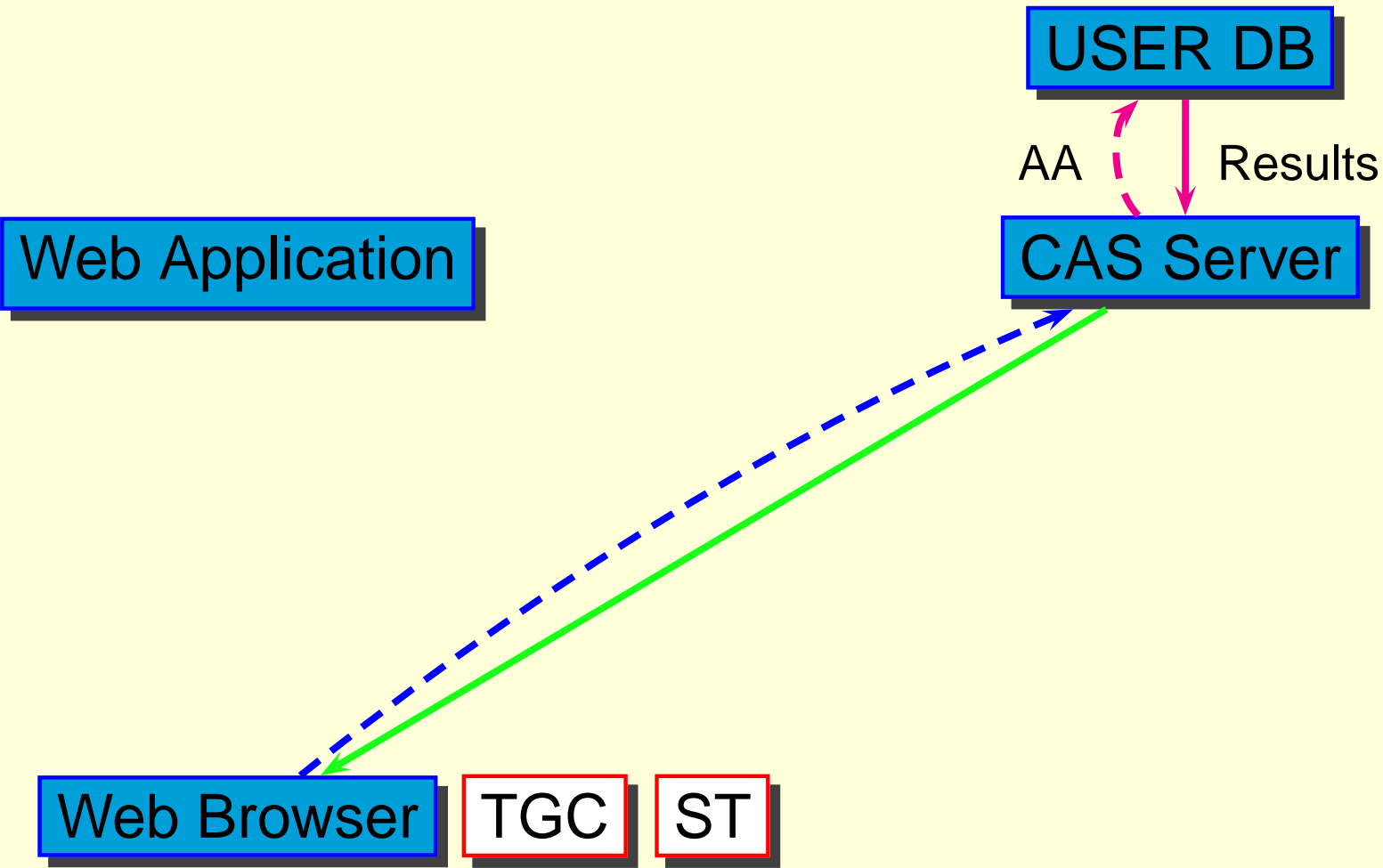
# Mechanism CAS and CAS2



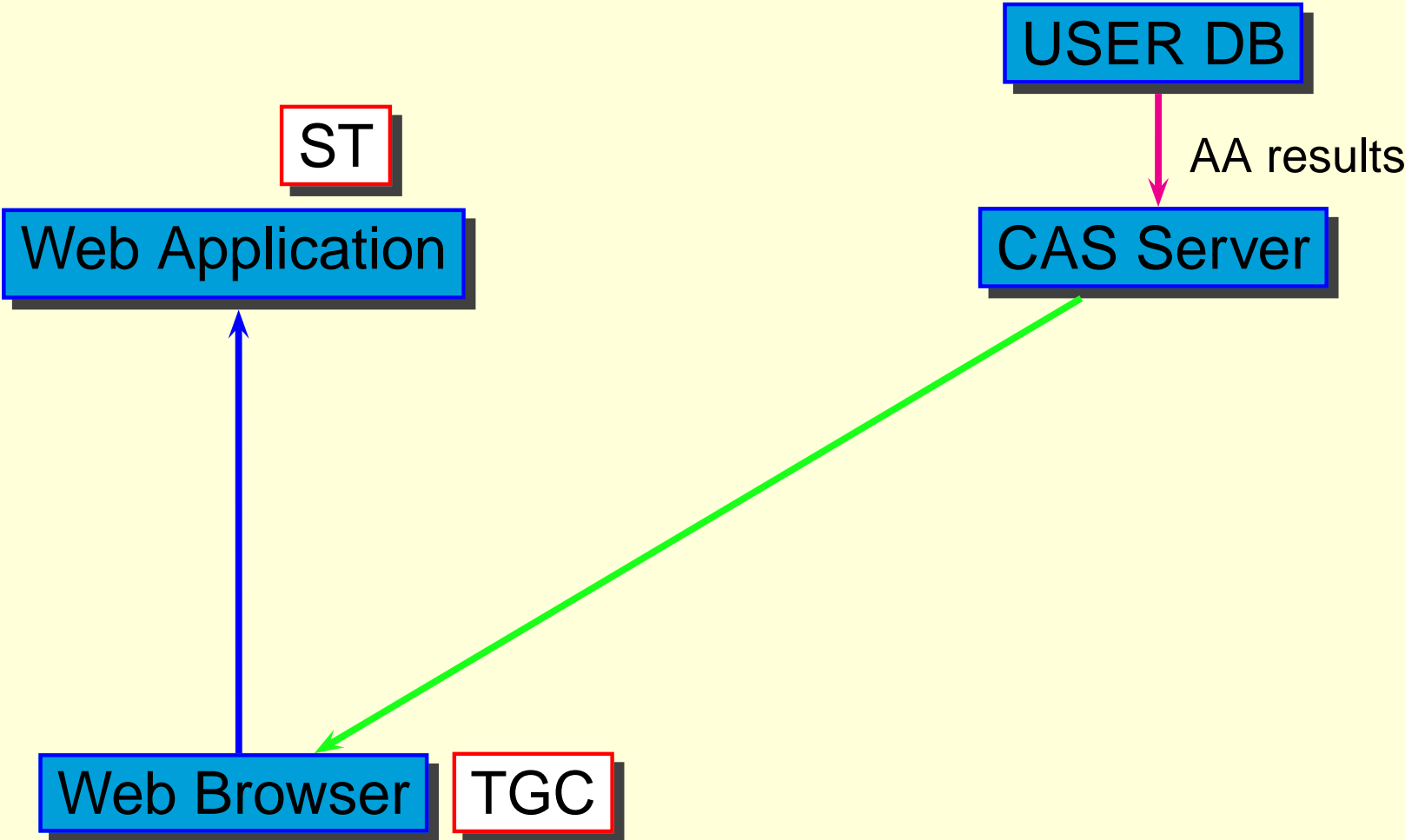
# Mechanism CAS and CAS2



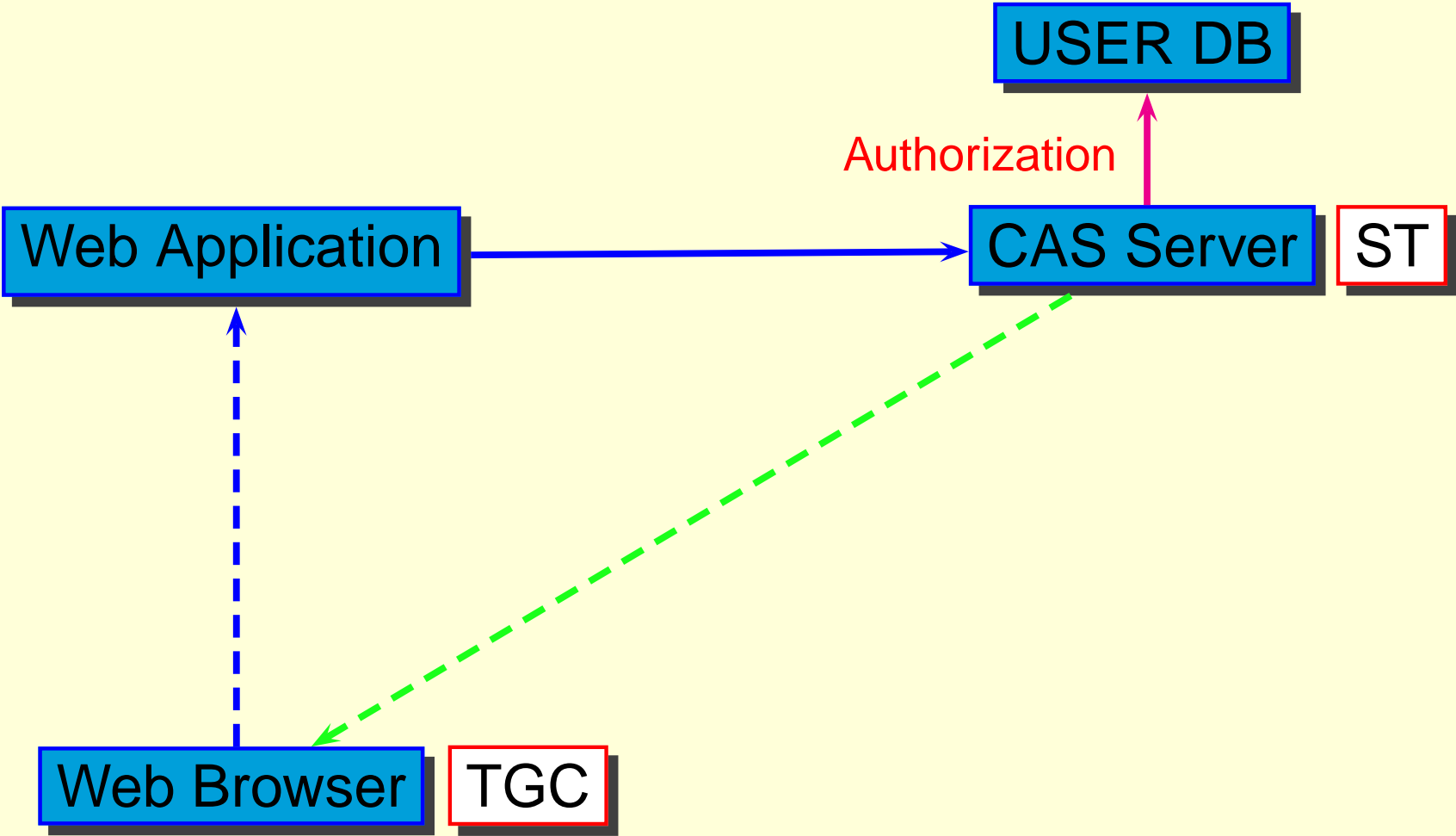
# Mechanism CAS and CAS2



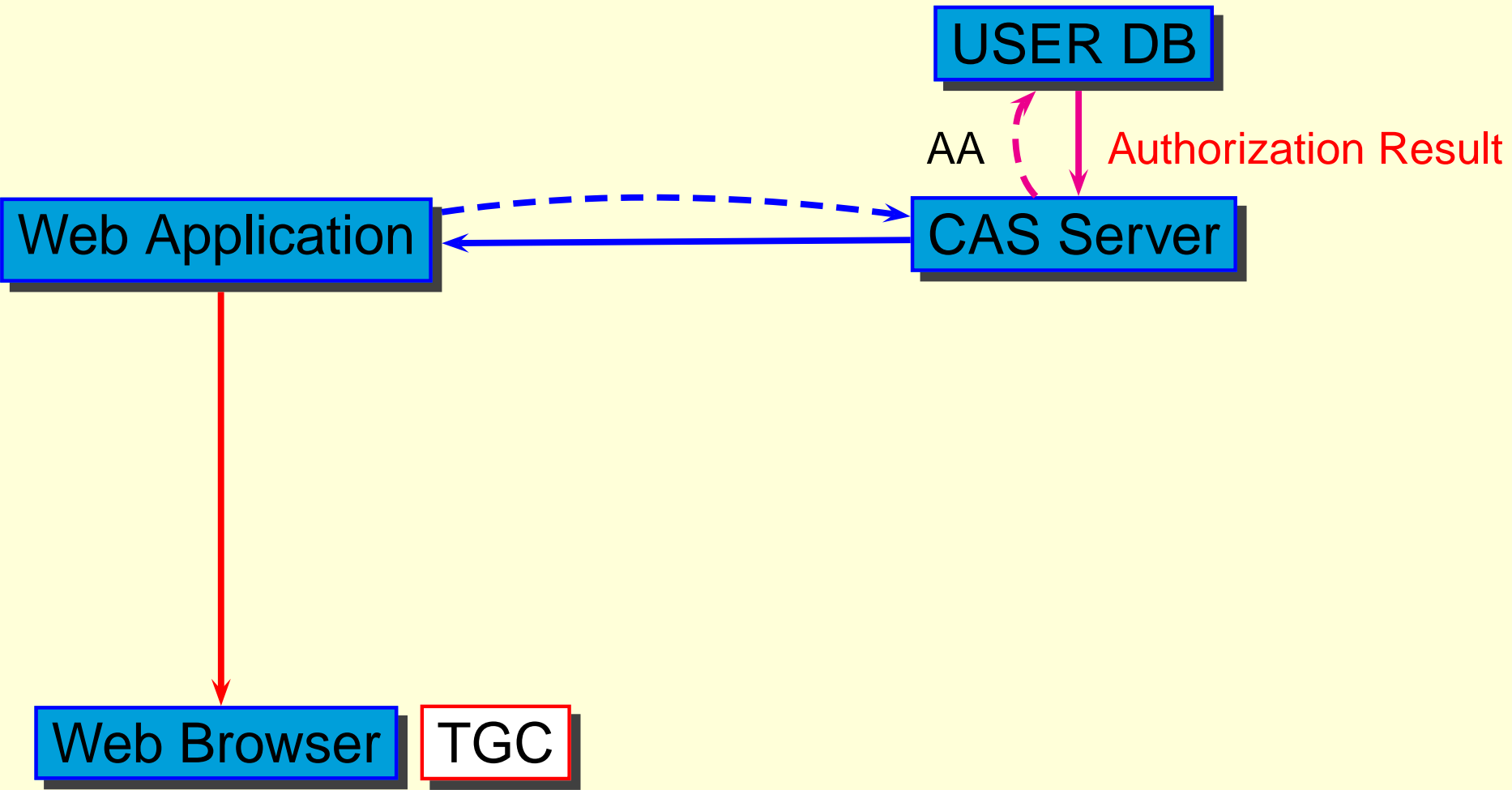
# Mechanism CAS and CAS2



# Mechanism CAS and CAS2



# Mechanism CAS and CAS2



# Mechanism CAS and CAS2

---

- Ticket Granting Cookie (TGC)
  - If Browser has TGC, Browser is Authenticated
- Service Ticket (ST)
  - One Time Ticket for accessing to Web Application
  - Including Authorization Information
  - If ST is valid, the access is Authorized

# Authorization Mechanism of CAS2

- Data Base for Authorization (CAS-ACL)
  - CAS-ACL is Access Permission Lists of
    - **FOR WHICH** Web Application (target URL)
    - **WHO** (User Information)
    - **WHEN** (Access Time)
    - **FROM WHERE** (Client Information)
- **ST** has an information that the access matches which entry of CAS-ACL

# Example of CAS-ACL

```
dn: cn=entry1,ou=gakumu,ou=cas,o=nagoyaUniv
cas-allow: (&(uid=naito)(date>=20051010)
(date<=20051110)(IP=133.6.130.0/24))
cas-service: https://app.*\.mynu\.jp/.*+
cas-attributes: uid,mailAddress,IdNo,FullName,dn
```

- When URL matches to `https://app.*\.mynu\.jp/.*+`
  - `uid` is `naito`
  - Access time is between **2005/10/10** and **2005/11/10**
  - Client IP: `133.6.130.0/24`then the access is granted.
- CAS Server send User information `uid,mailAddress,IdNo,FullName,dn` to the Web Application

# CAS2 in Nagoya University

- Web Applications using CAS<sup>2</sup> in Nagoya University
  - Nagoya University Portal
  - Course Registration System
    - 10000 Students and 2000 Faculties
  - Researcher Database
    - 2000 Faculties
  - Web CT
  - ...
- These Applications are
  - Single Sign On
  - Access Controledby CAS<sup>2</sup>

# Summary

---

- CAS<sup>2</sup> is easy to use:
  - Easy to construct **Single Sign On** Environment
  - Easy to construct **Unified Authorization** Environment
  - Easy to modify Application to use CAS: Only modify to use **CAS client** module for Authentication and Authorization
  - ONLY SSL for encryption
- CAS<sup>2</sup> is secure:
  - Web Application does not handle Authentication Information
  - Web Application does not directly access to USER DB