Single Sign On and Authorization Infrastructure using CAS^2

Shoji KAJITA (Information Technology Center, Nagoya University)

and

Hisashi NAITO (Graduate School of Mathematics, Nagoya University)

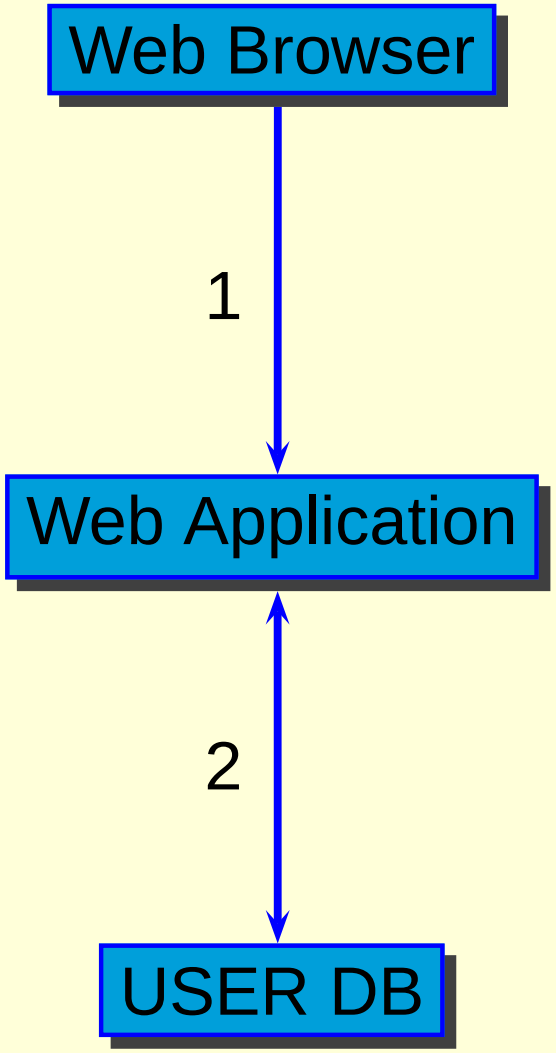
Plan of Talk

- Short introduction for CAS and CAS^2
- Authentication mechanism of CAS and Authorization mechanism of CAS^2
- "Nagoya University Portal" using CAS^2
- Summary

What is CAS & CAS2

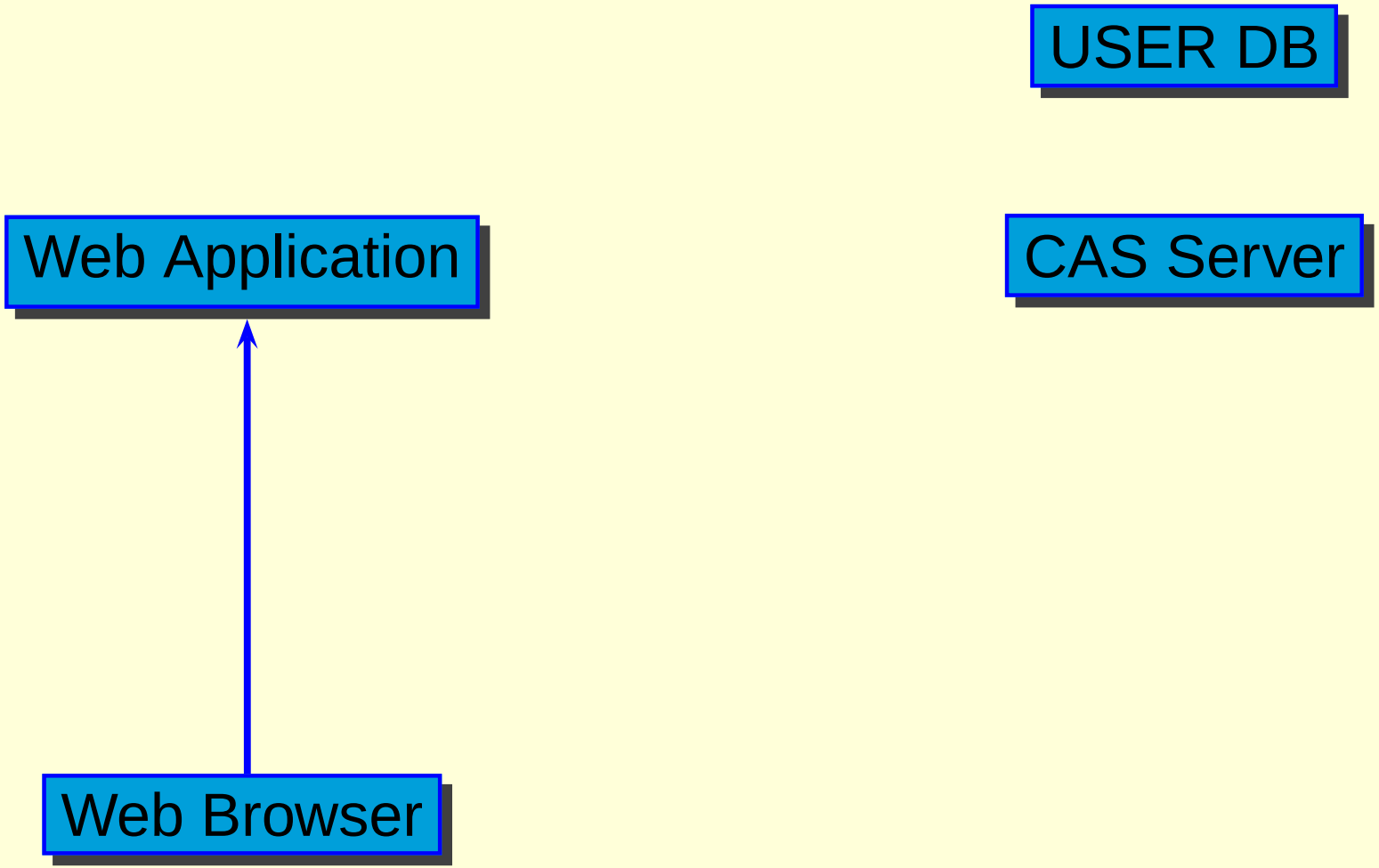
- CAS
  - Single Sign On Environment for Web Applications
  - Open Source software depeloped by Yale University
- CAS^2
  - We extends to Authorization Environment for Web Applications
  - CAS^2 controls Access Rights for each Web Application
    - WHO
    - WHEN
    - from WHERE

Usual Authentication and Authorization

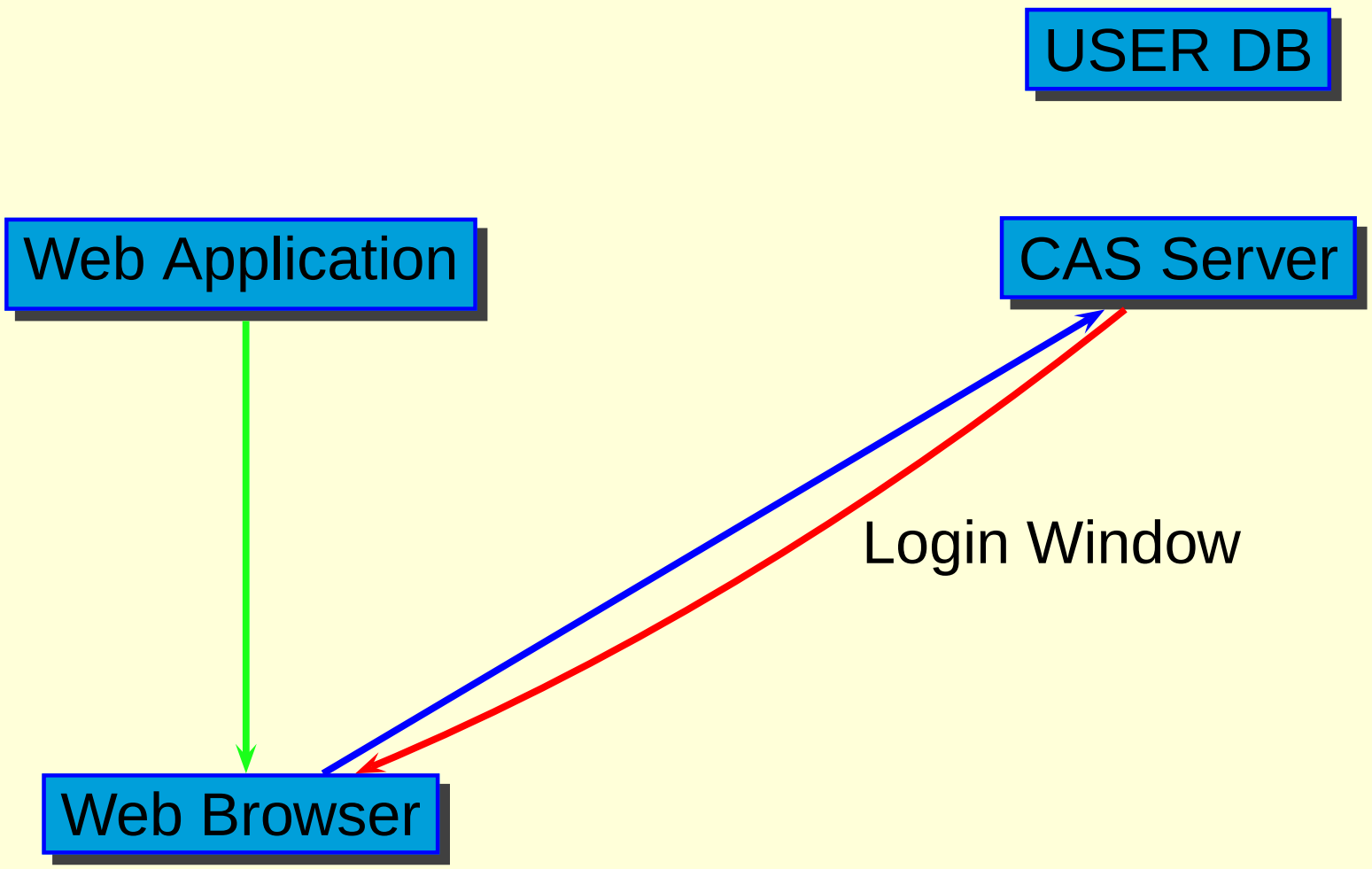


- Web Application must includes AuthN & AuthZ codes
- Web Application directly accesses to USER DB to obtain User Informations
  - Web Application has a password to access to USER DB

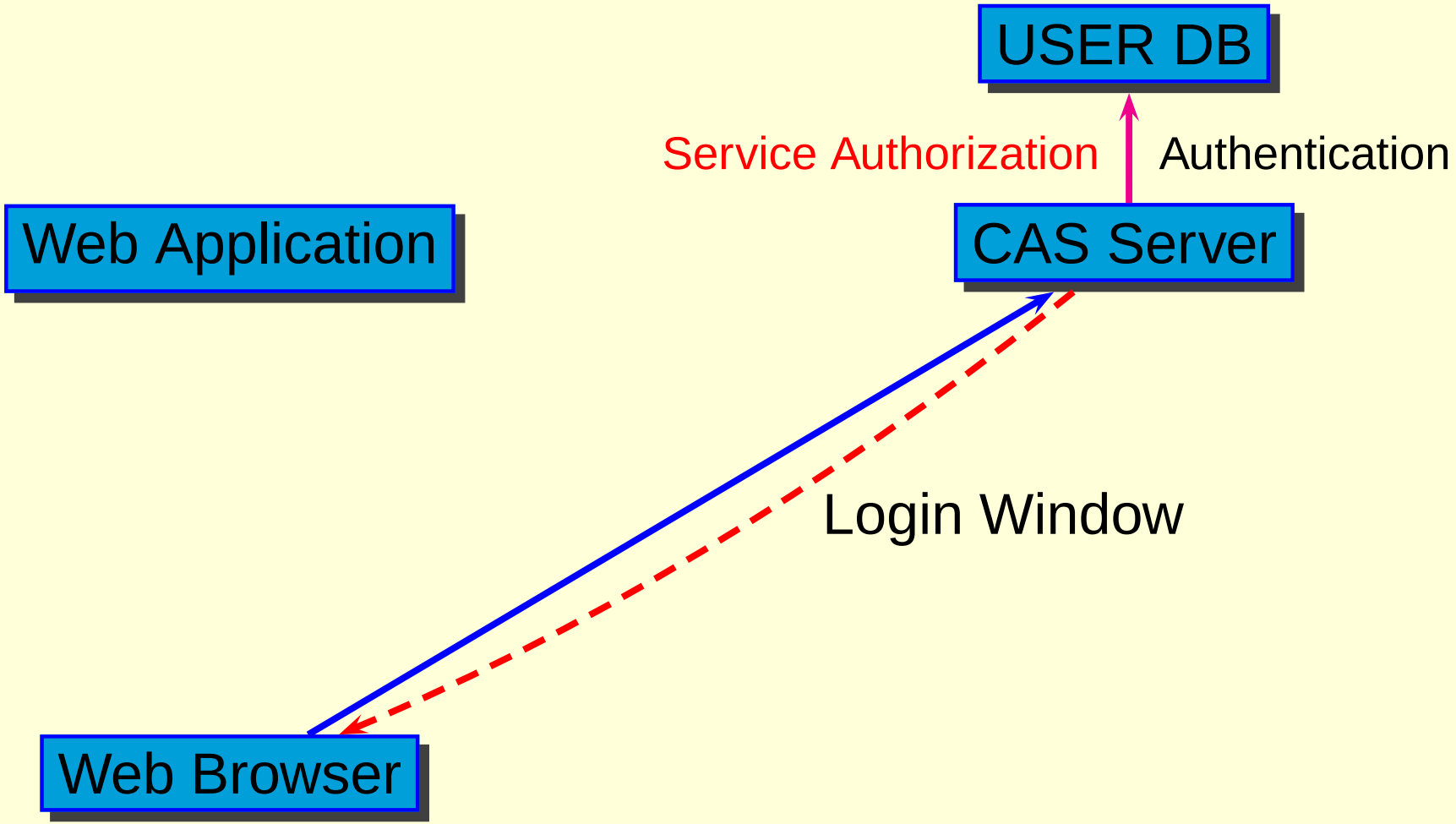
Mechanism CAS and CAS2



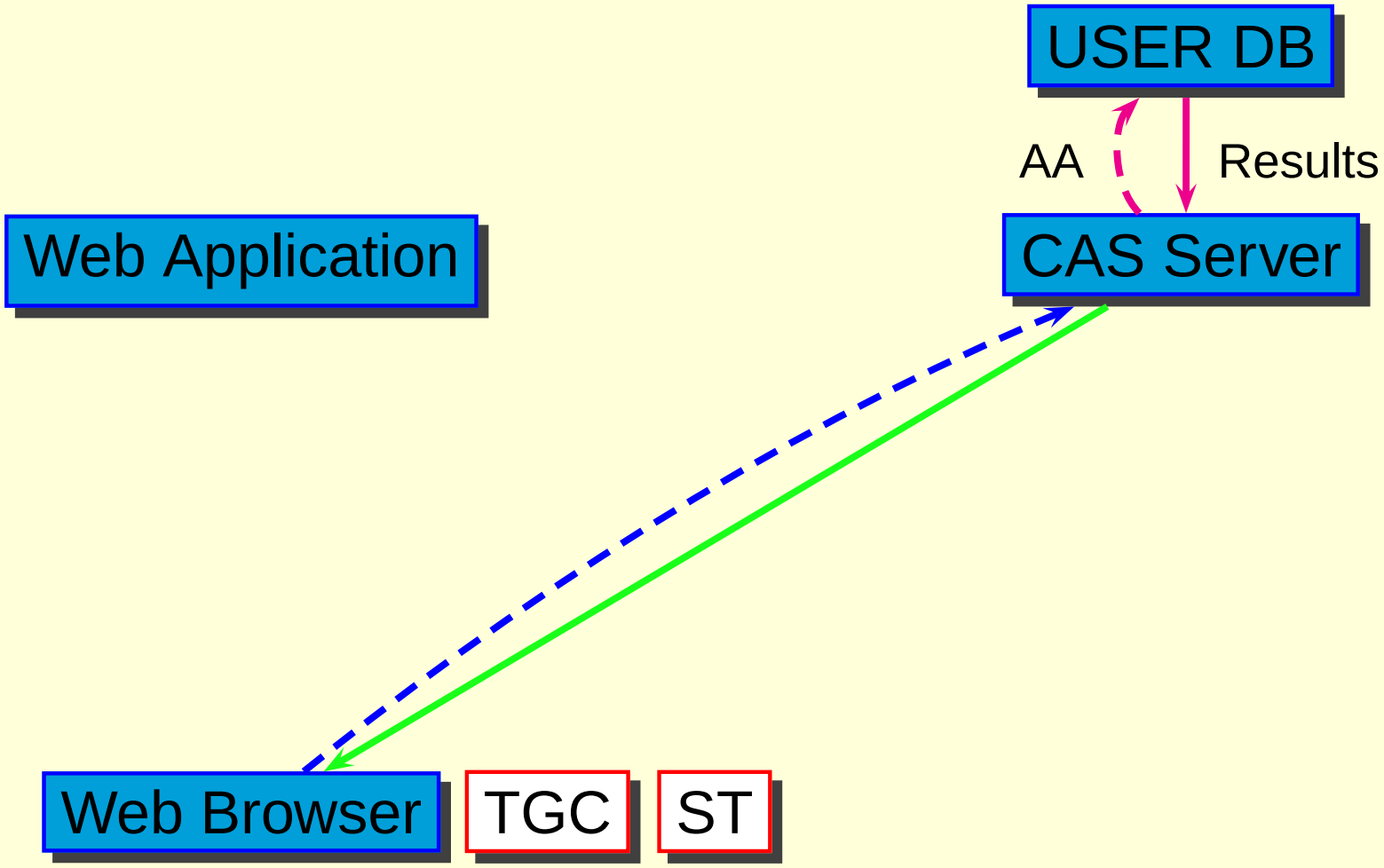
Mechanism CAS and CAS2



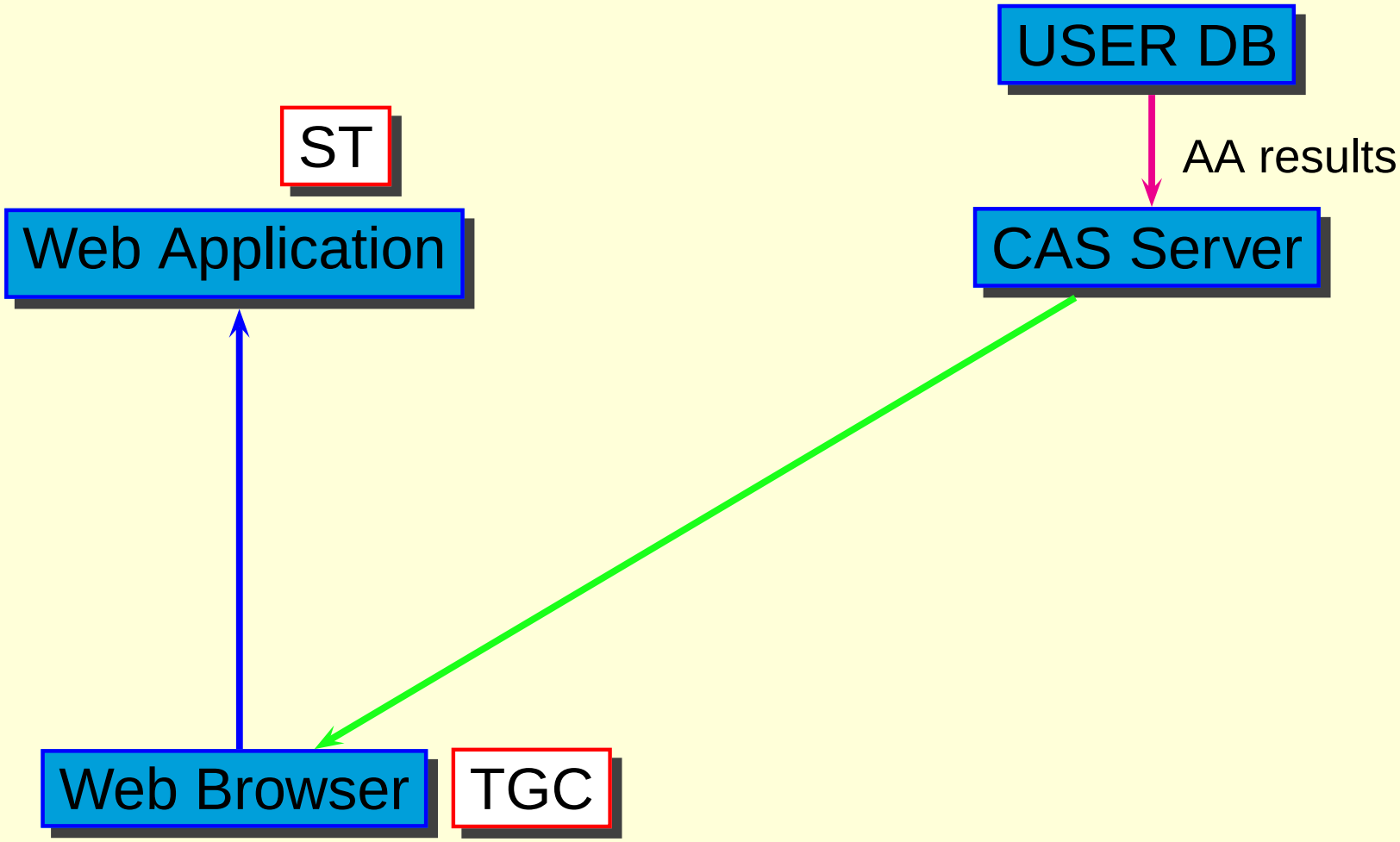
Mechanism CAS and CAS2



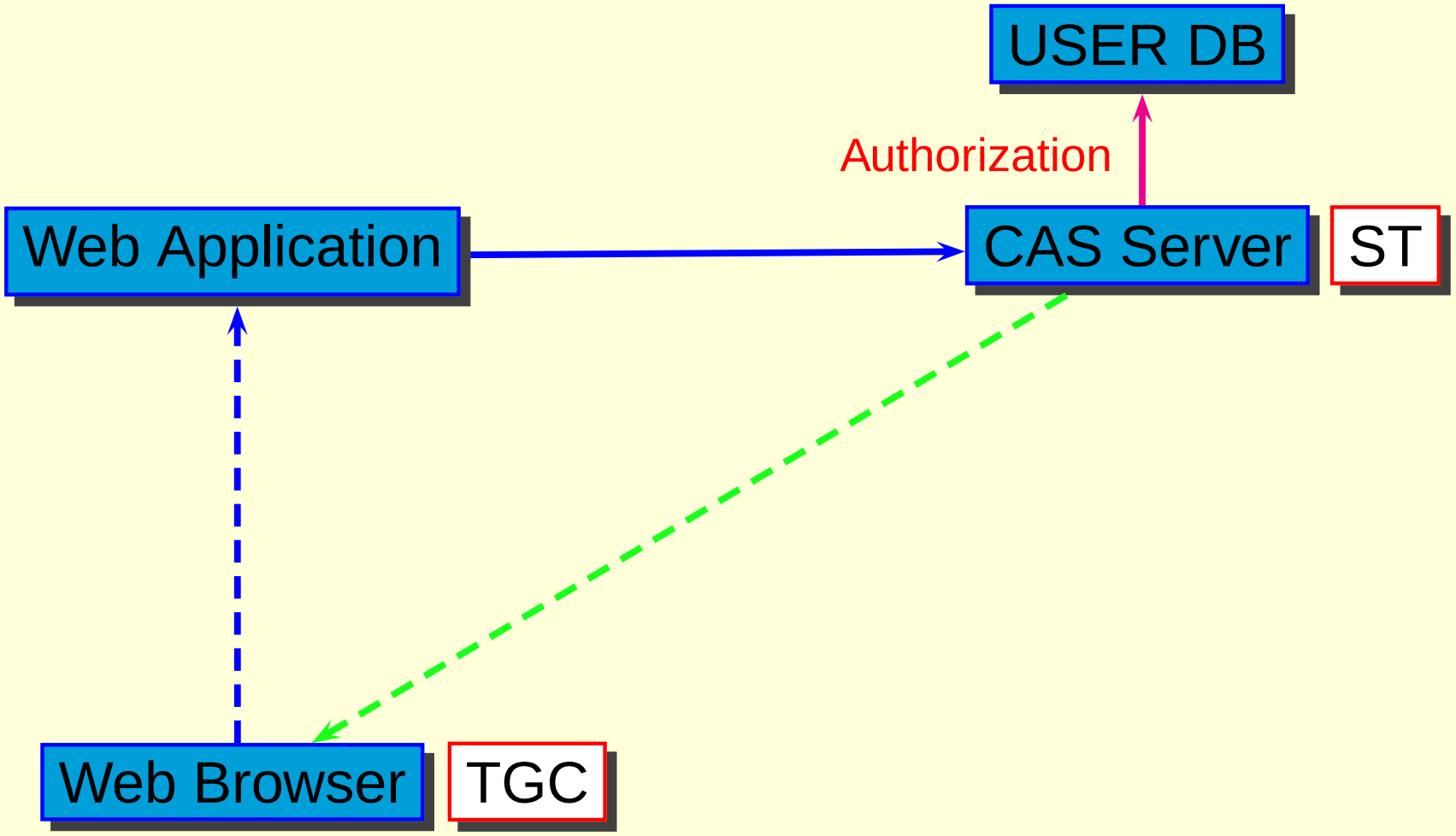
Mechanism CAS and CAS2



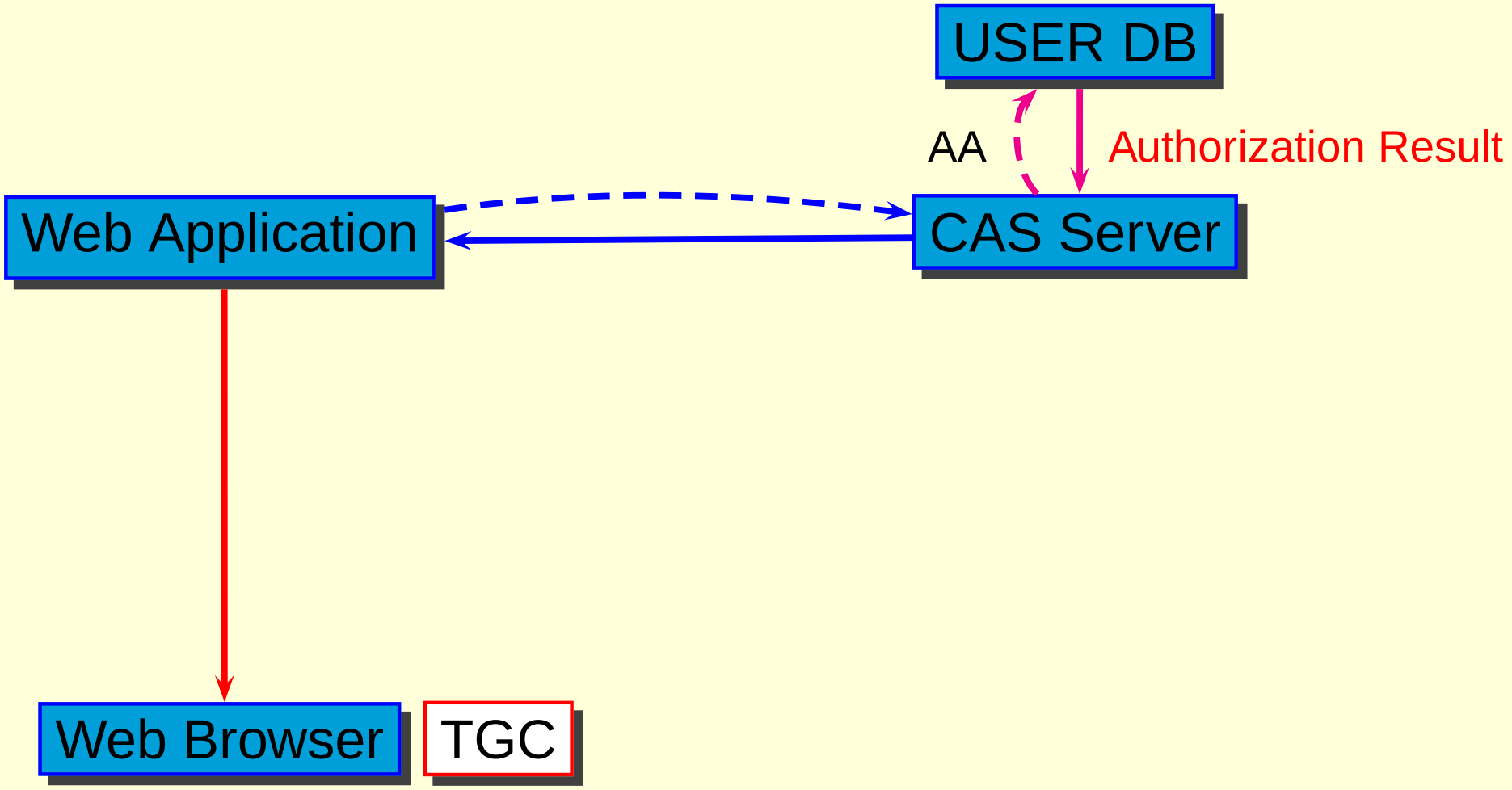
Mechanism CAS and CAS2



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 Mechanisum 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^2 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 Controled

  by CAS^2

Summary

- CAS^2 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 Autorization
  - ONLY SSL for encryption
- CAS^2 is secure:
  - Web Application does not handle Authentication Information
  - Web Application does not directly access to USER DB