Pour aller plus loin avec CAS

Jérôme Leleu – 6 février 2014 – ESUP days

1. Moi
2. CAS
3. Authentification multi-facteurs
4. Déconnexion
5. Mobile

Groupe de travail ESUP sur l’authentification

Responsable technique chez SFR

Chairman CAS

@leleuj

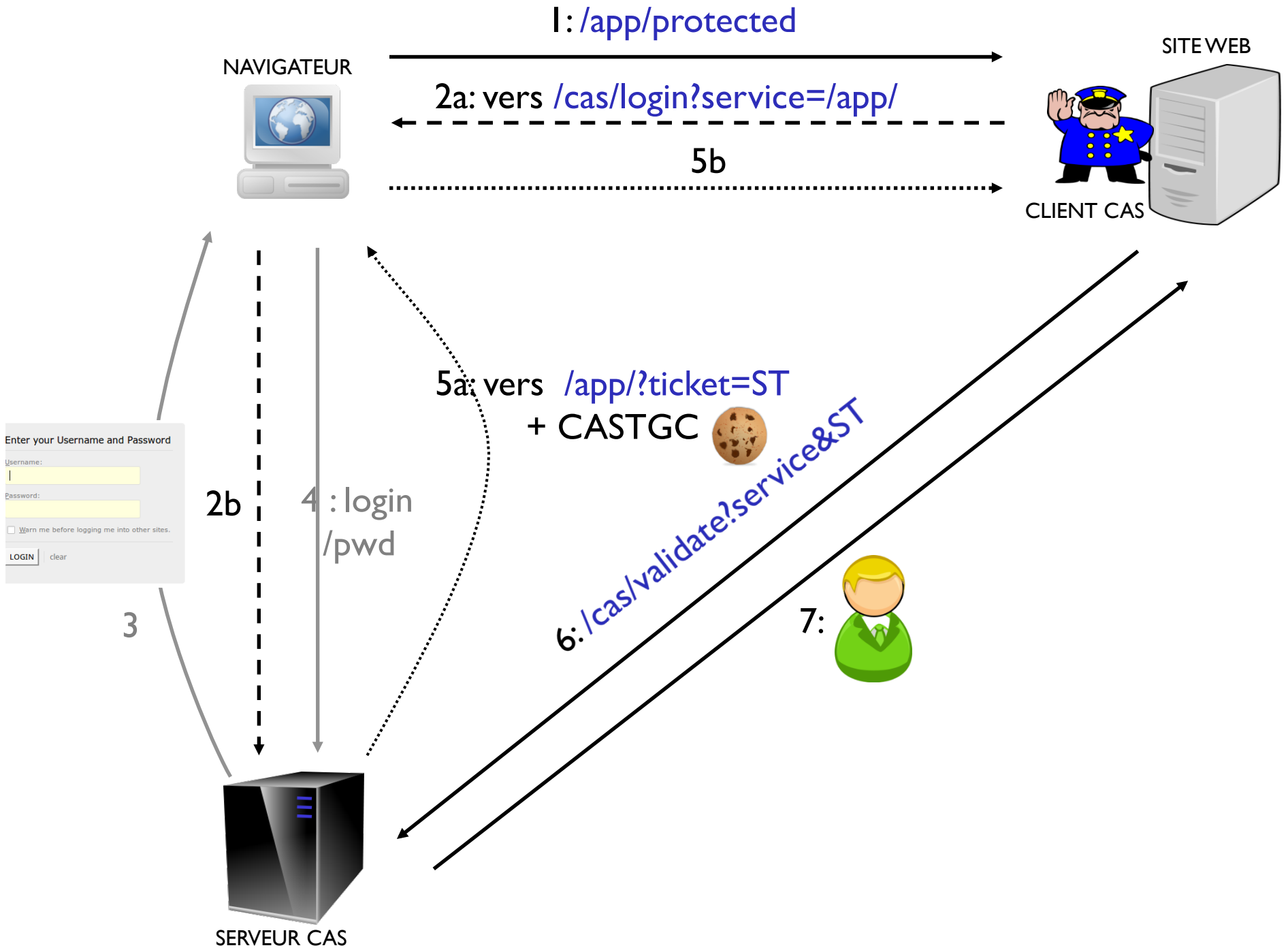
https://github.com/leleuj


CAS

SSO web

Projet open source créé à Yale en 2001

Communauté active, 7 committers


1: /app/protected
NAVIGATEUR
SITE WEB
2a: vers /cas/login?service=/app/
5b
CLIENT CAS
5a: vers /app/?ticket=ST
+ CASTGC
Enter your Username and Password
Username:
Password:
Warn me before logging me into other sites.
LOGIN
clear
2b
4 : login
/pwd
3
6: /cas/validate?service&ST
7:
SERVEUR CAS

1. Serveur performant en Java

2. Des clients en Java, .Net, PHP…

3. Un protocole simple et puissant

Back office d’administration

Interopérabilité avec OAuth, OpenID, SAML

Déconnexion centralisée

API REST, remember-me, LPPE, ClearPass…

Multi-facteurs ≠ forte ≠ faible

≥ 2 preuves (*credentials*)

Sécurité

Grille par utilisateur, code supplémentaire envoyé par SMS / email, clé SecurID...

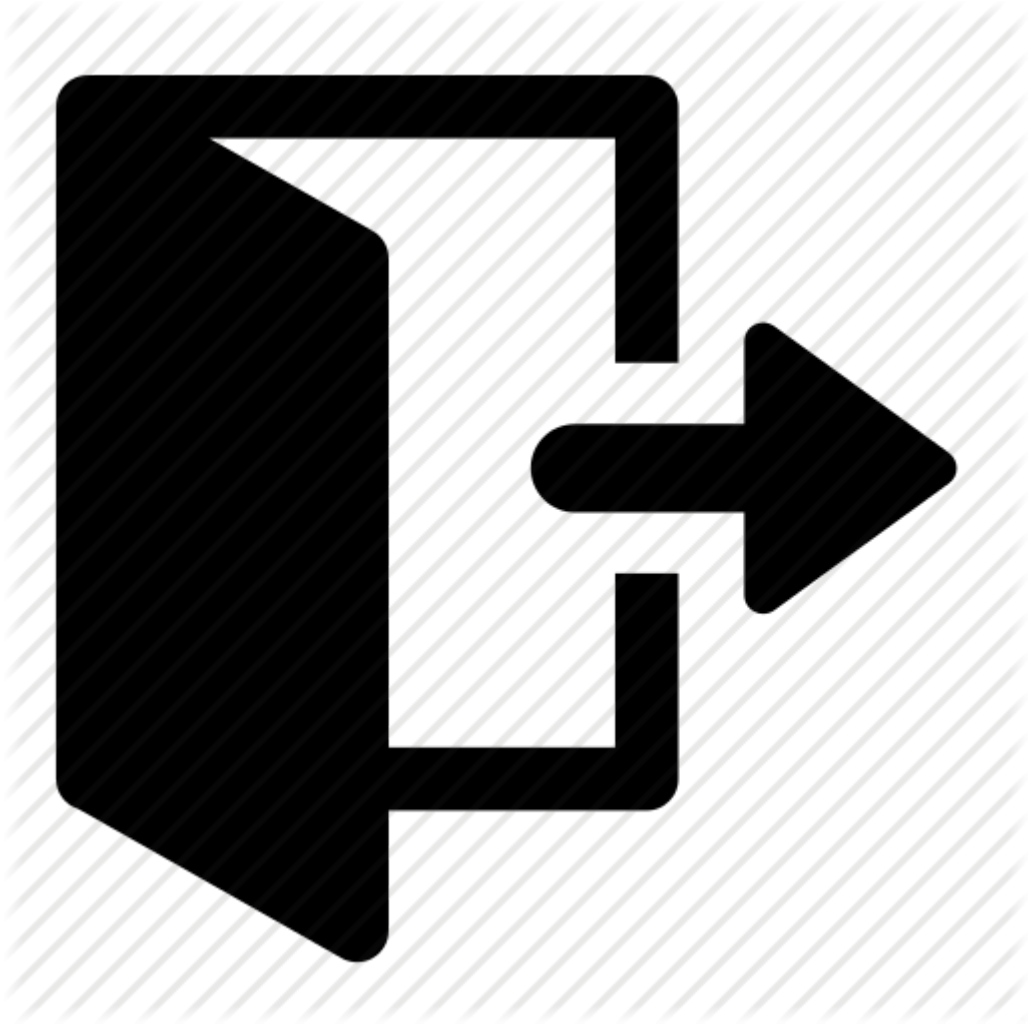
Version	UI	une authentification =	Accès à un service
3.5.x	*login / password*	1 *principal*	Si authentifié
4.0	*login / password*	1 *principal* + N *authentication handlers* ok	Si authentifié
4.x / 5 ?	N *credentials*	1 *principal* + N *authentication handlers* ok	Si le bon niveau de sécurité (N *authentication handlers* ok)

Level Of Assurance

Implémentations possibles :

1. Customisation du serveur CAS :
   - UI
   - *authentication handler/manager*
   - *GenerateServiceTicketAction*

2. Chaînage de serveurs CAS (J. Marchal) :
   - 1 serveur CAS *classique*
   - 1 serveur CAS *renforcé* protégé par le serveur *classique*



LOGOUT

SLO = Single Log Out

Ergonomie / fonctionnel

Back channel

Problèmes :

- clustering et affinité de session
- applications CAS ne supportant pas le logout
- installation multi SSO

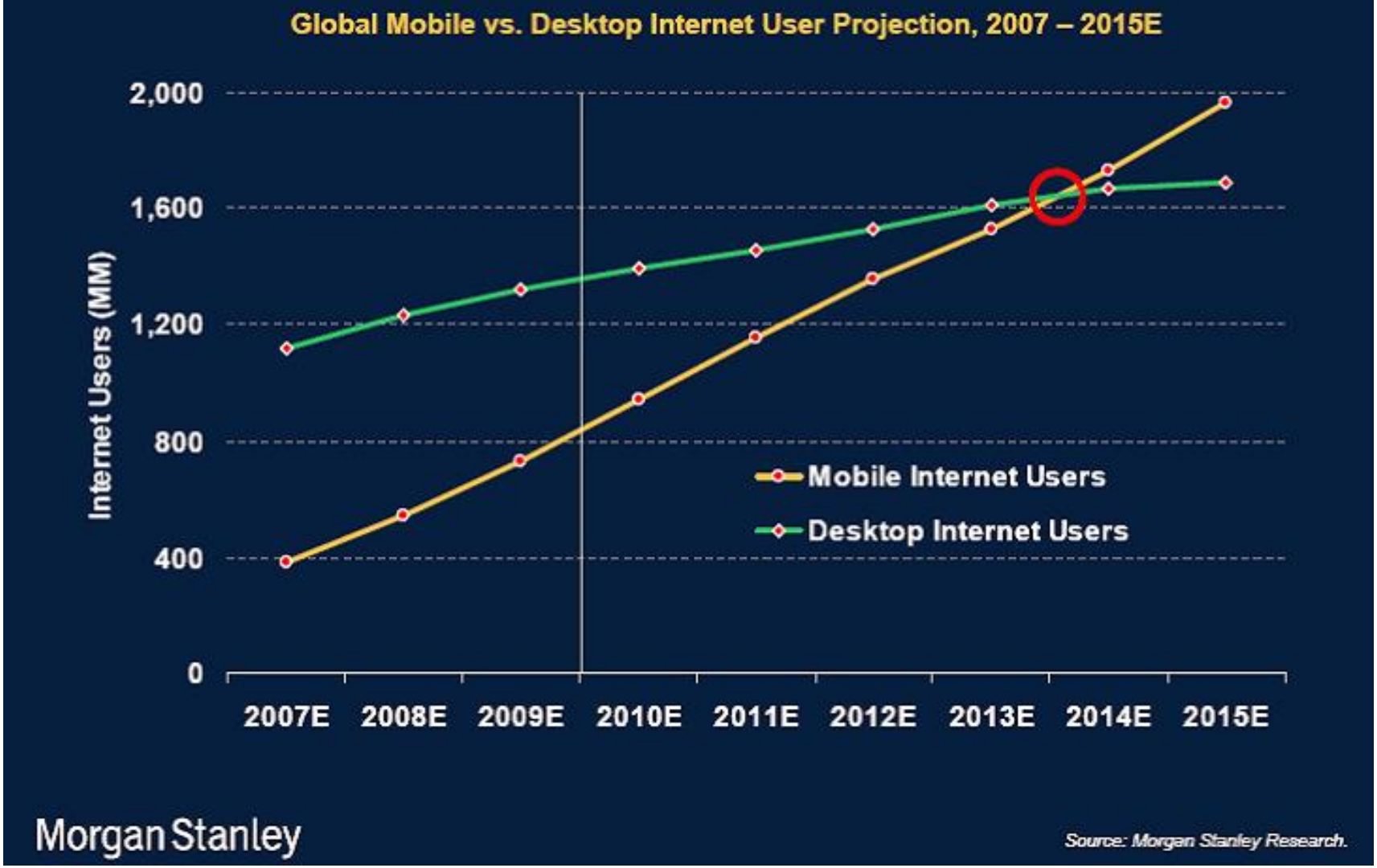
CAS 4.0 : SLO *front channel* expérimental

Customisations de la page de logout :

- iframes / images cachées
- Javascript
- proxy


SFR

Mobile Users > Desktop Internet Users Within 5 Years



Morgan Stanley

Source: Morgan Stanley Research.

Applications web sur mobile :

Solutions pour un rendu adapté :

- configuration possible du thème CAS
- page de login *responsive design*

Limitation de la fréquence d'authentification : remember-me CAS

Applications mobiles :

~~SSO web~~

Validation des login/password :

- API REST de CAS
- web service custom

Limitation de la fréquence d'authentification : stockage local d'un token ? -> OAuth

Feedbacks et propositions très intéressants

CAS : "bel effort, doit persévérer"