Certificate Transparency : des journaux publics en ajout seul pour sécuriser TLS

Florian Maury (ANSSI)

15 décembre 2016

Rappel du contexte

Des centaines d'autorités de certification :

- nombreux rapports d'incident (émissions non-sollicitées ou certificats invalides : Comodo, Diginotar, CNNIC, Symantec. . .)

Solutions possibles :

- **changer** de système de confiance ?
- **renforcer** les exigences ?
- **détecter** les anomalies ?

Rappel du contexte

Des centaines d'autorités de certification :

- nombreux rapports d'incident (émissions non-sollicitées ou certificats invalides : Comodo, Diginotar, CNNIC, Symantec. . .)

Solutions possibles :

- ✓ **changer** de système de confiance ?
- ✓ **renforcer** les exigences ?
- ✓ **détecter** les anomalies ?

Journaliser les certificats émis

Journalisation publique des certificats émis :

- base de données classique **inadaptée**
  - propriétés d'intégrité trop faibles

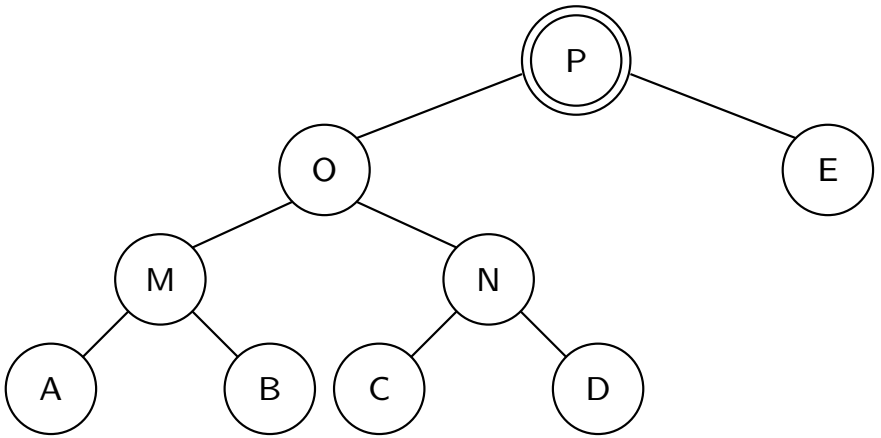
Propriétés attendues :

- **en ajout seul**
- **vérifications efficaces**

Structure d'un journal en ajout seul

Repose sur les **fonctions de hachage cryptographiques** (e.g. SHA-2) :

- arbre de Merkle (1979)



Exemples d'usage : Git, Bitcoin

Certificate Transparency

Des journaux de certificats pour TLS

Principe général de Certificate Transparency (CT)

IETF :

- RFC 6962
- WG *trans* : *draft* rfc-6962-bis-21

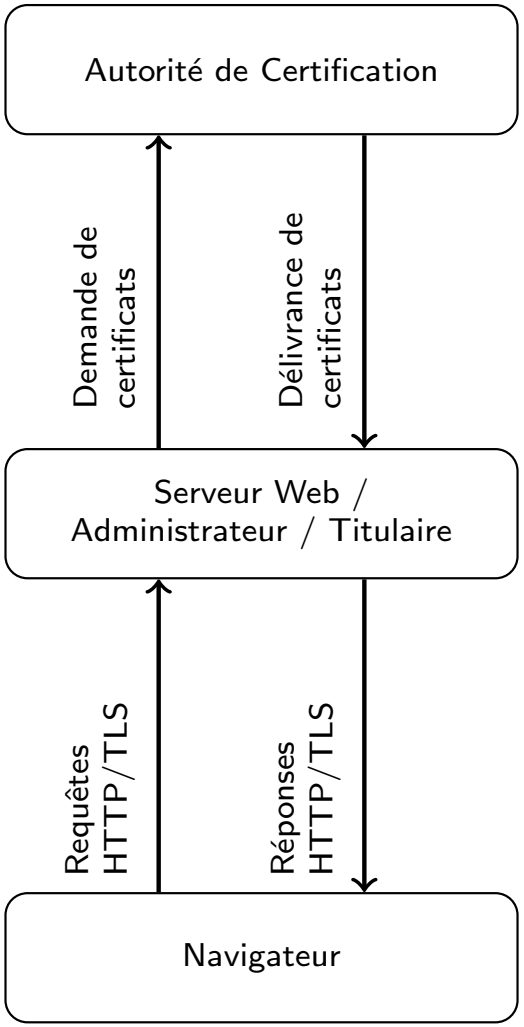
Objectifs :

- **journaliser les certificats** émis par les autorités de certification (AC) **publiques**
- permettre la **détection** des émissions défectueuses, frauduleuses ou indésirables
- ~~prévenir les interceptions TLS~~

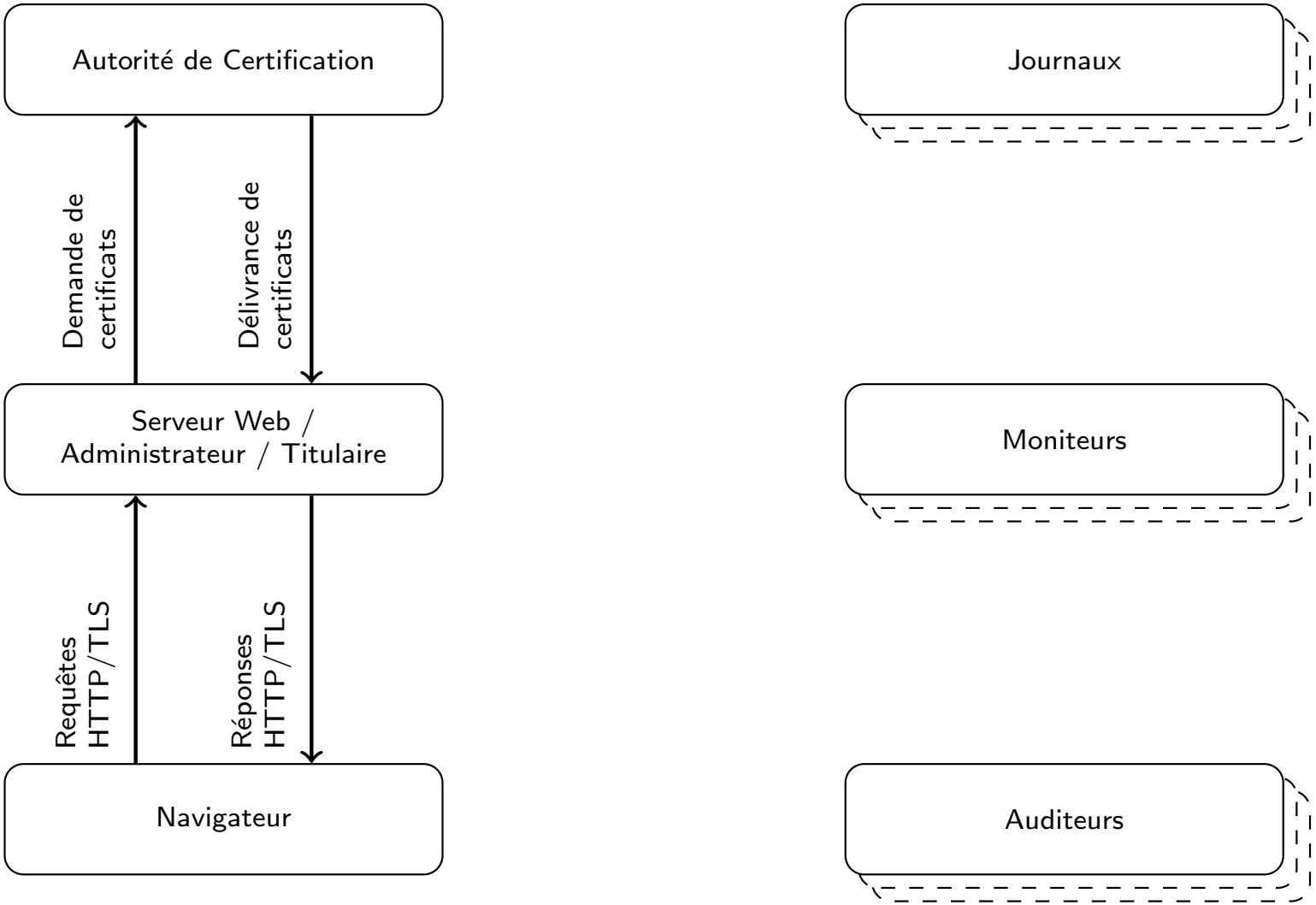
Certificate Transparency (CT) :

le synoptique théorique

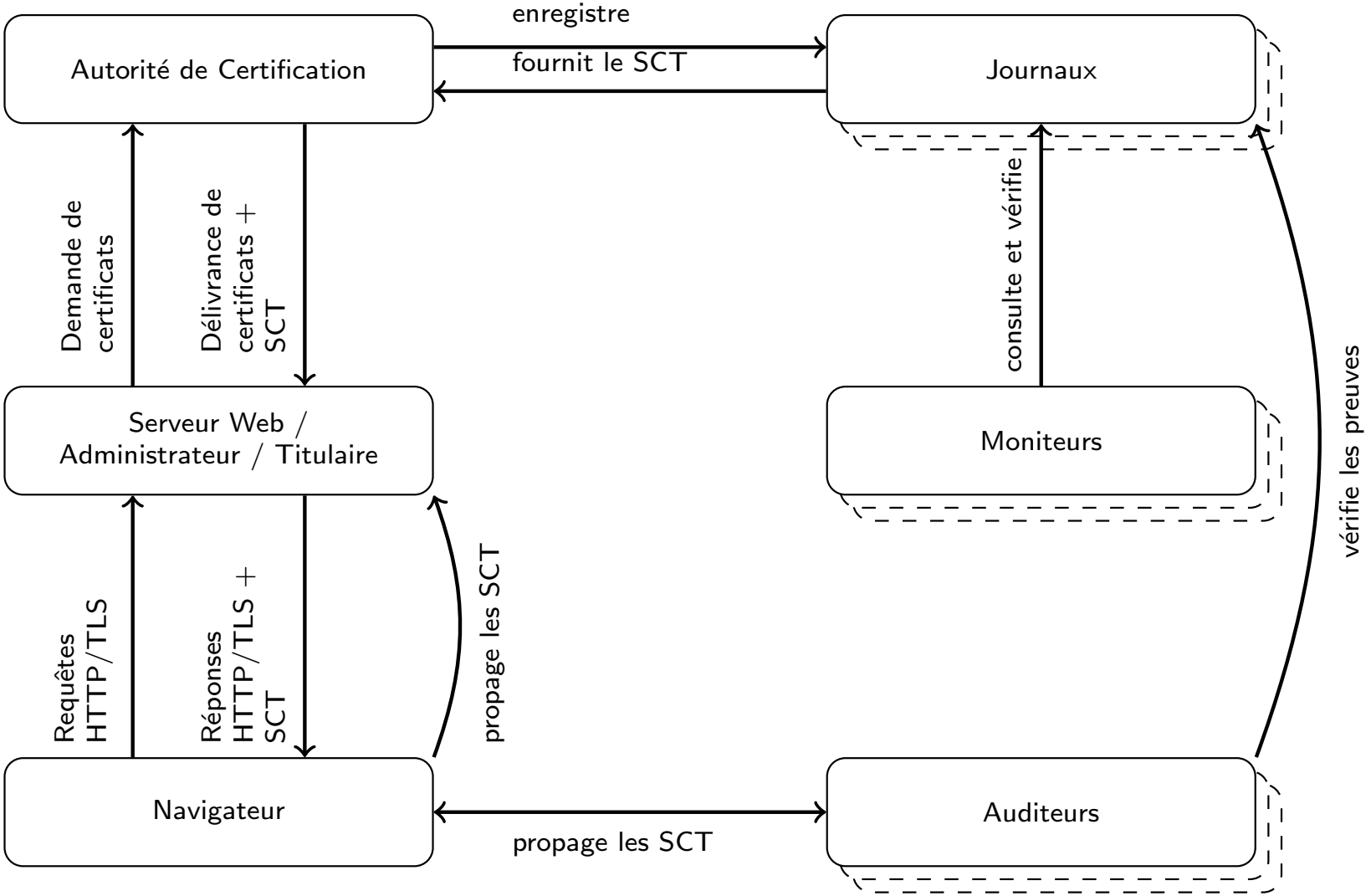
Relations entre les acteurs



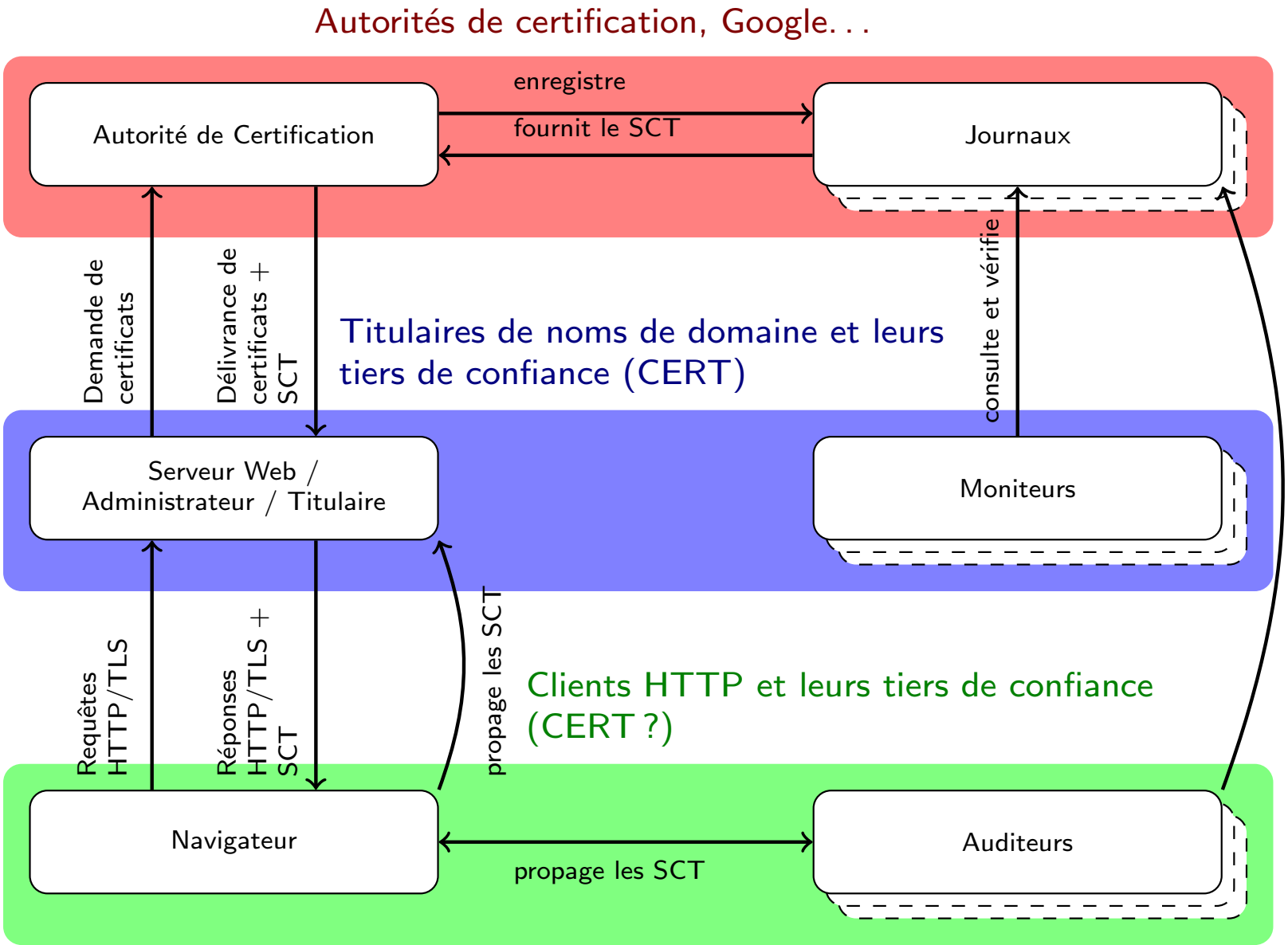
Relations entre les acteurs



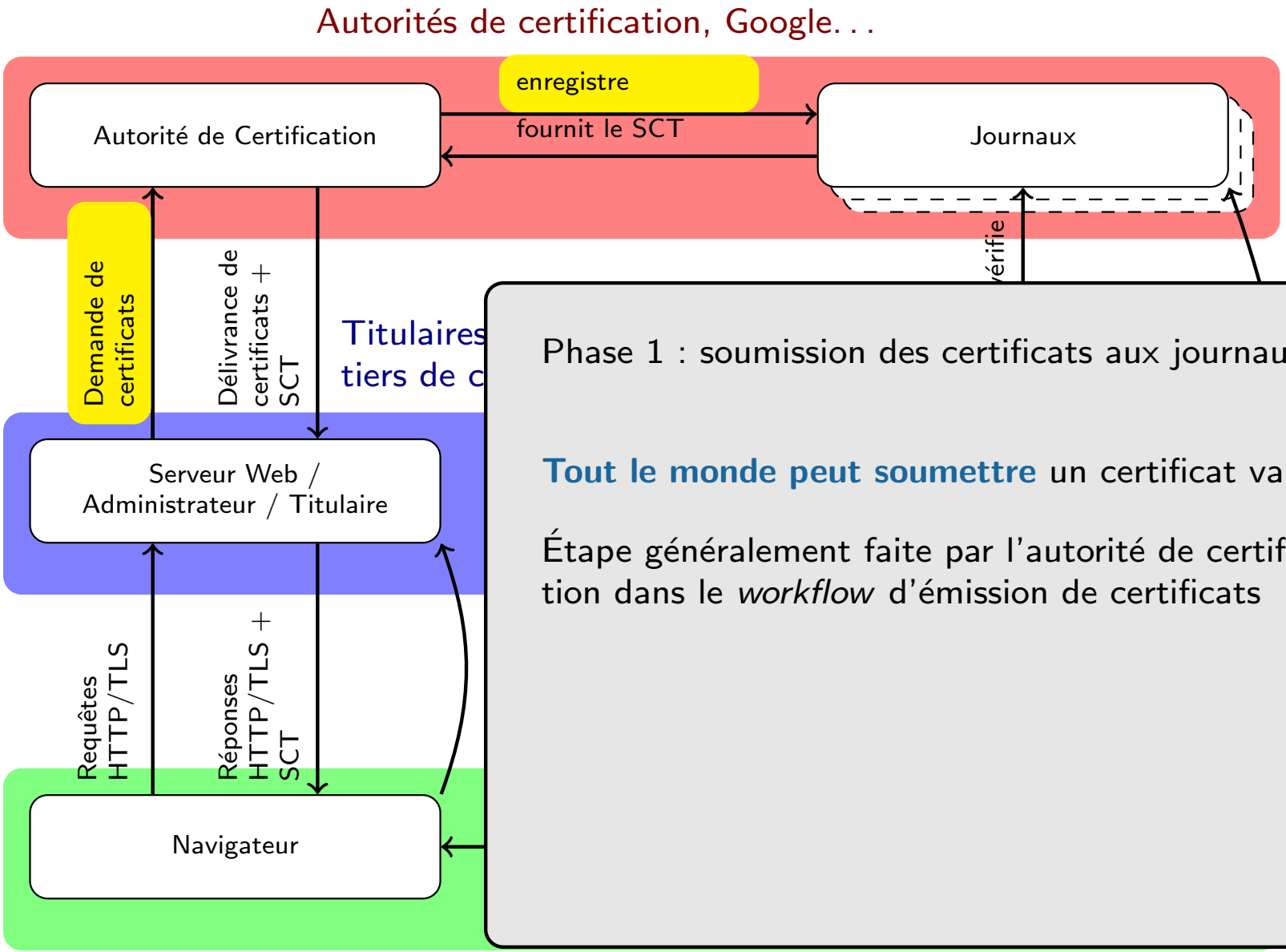
Relations entre les acteurs



Relations entre les acteurs



Relations entre les acteurs

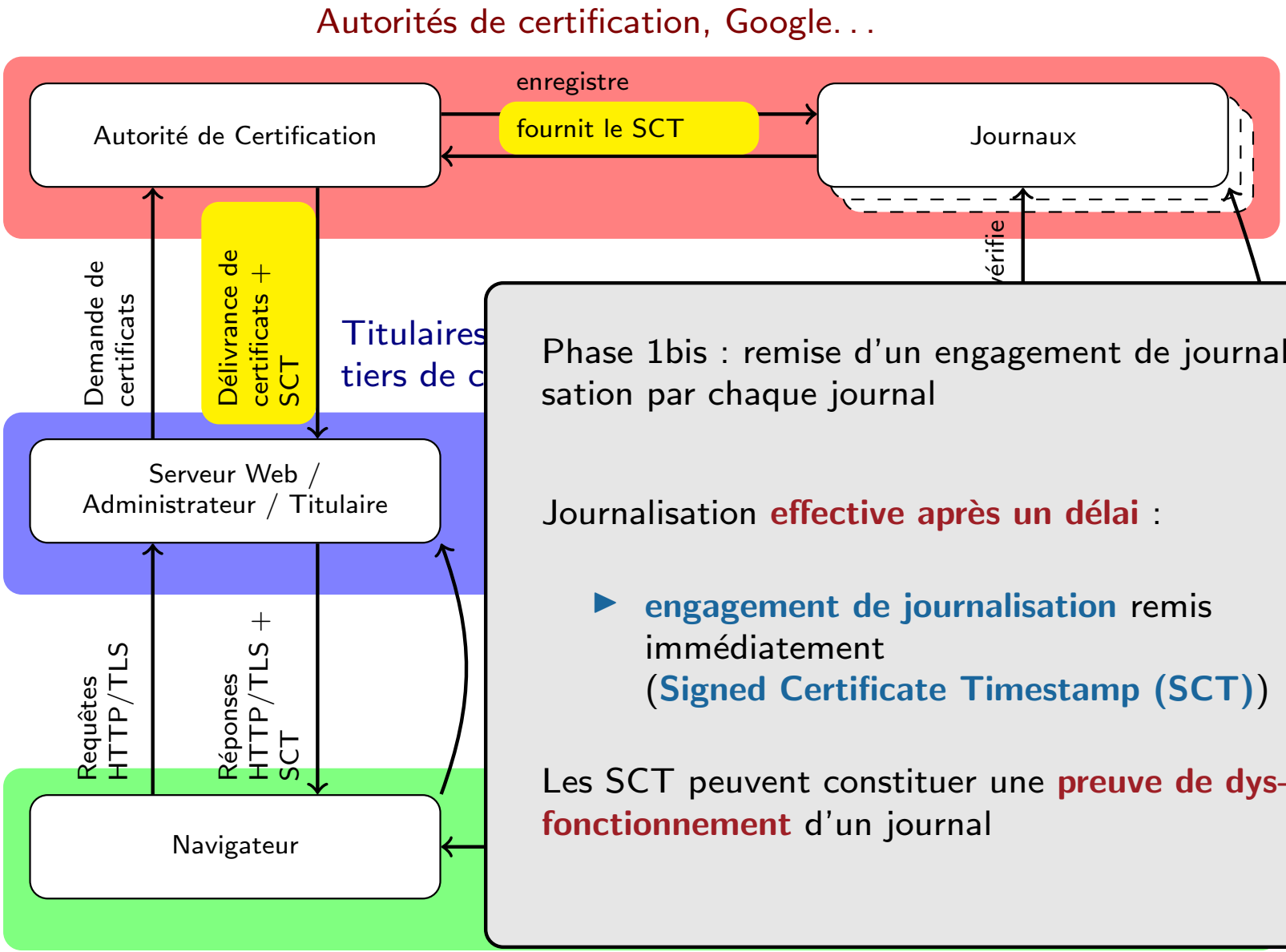


Phase 1 : soumission des certificats aux journaux

Tout le monde peut soumettre un certificat valide

Étape généralement faite par l'autorité de certification dans le *workflow* d'émission de certificats

Relations entre les acteurs



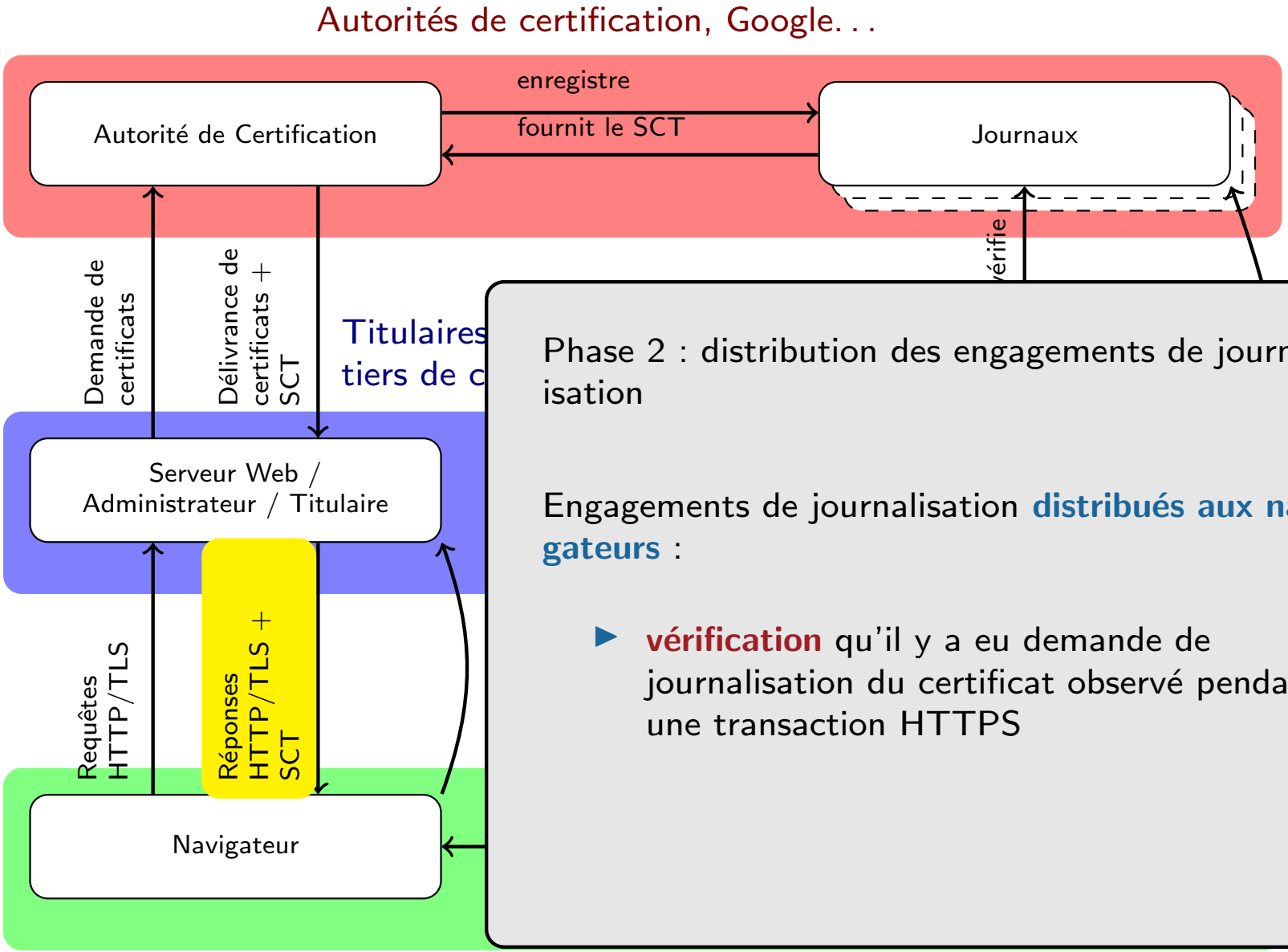
Phase 1bis : remise d'un engagement de journalisation par chaque journal

Journalisation **effective après un délai** :

- **engagement de journalisation** remis immédiatement (**Signed Certificate Timestamp (SCT)**)

Les SCT peuvent constituer une **preuve de dysfonctionnement** d'un journal

Relations entre les acteurs

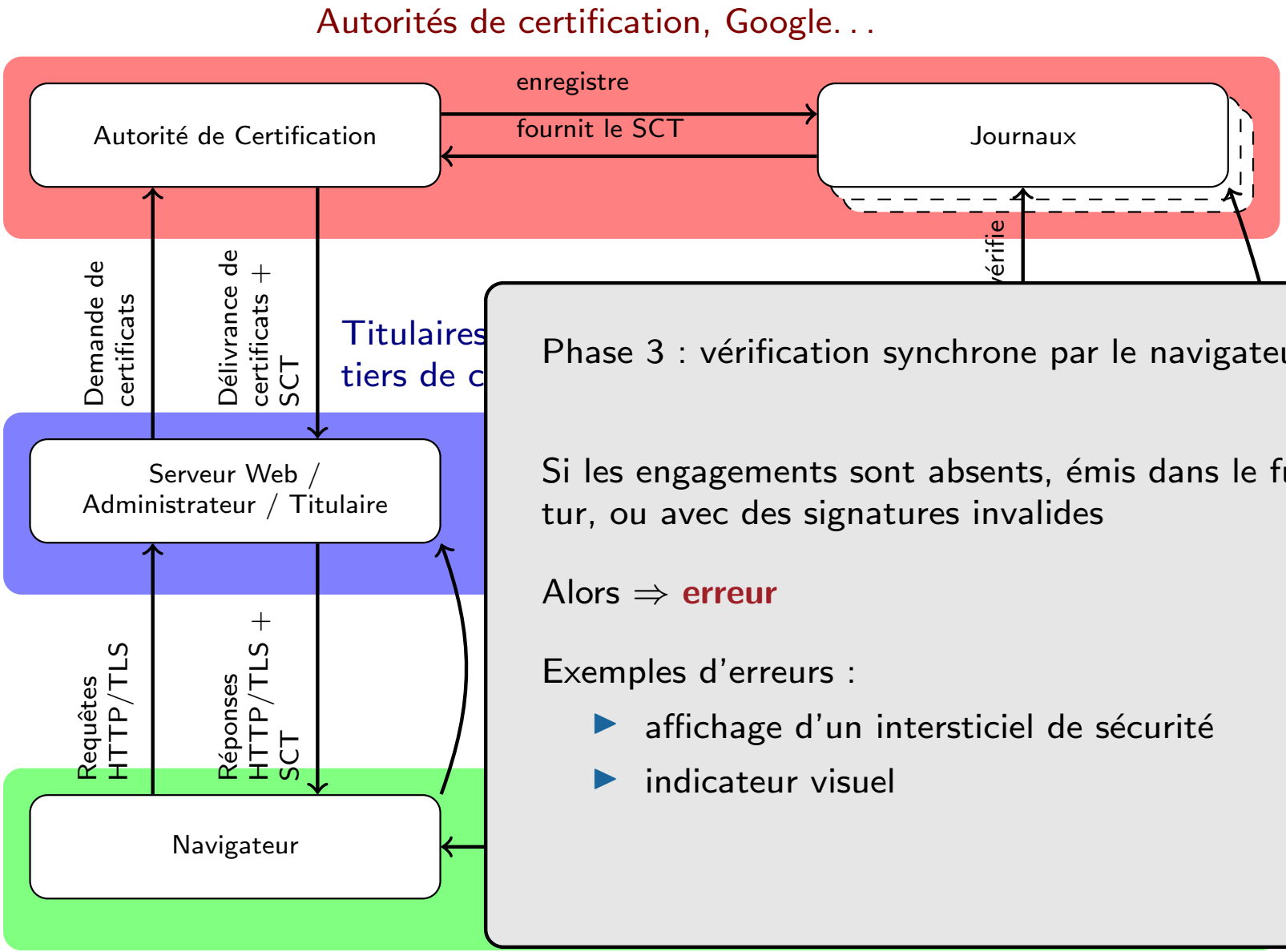


Phase 2 : distribution des engagements de journalisation

Engagements de journalisation **distribués aux navigateurs** :

- **vérification** qu'il y a eu demande de journalisation du certificat observé pendant une transaction HTTPS

Relations entre les acteurs



Phase 3 : vérification synchrone par le navigateur

Si les engagements sont absents, émis dans le futur, ou avec des signatures invalides

Alors ⇒ **erreur**

Exemples d'erreurs :

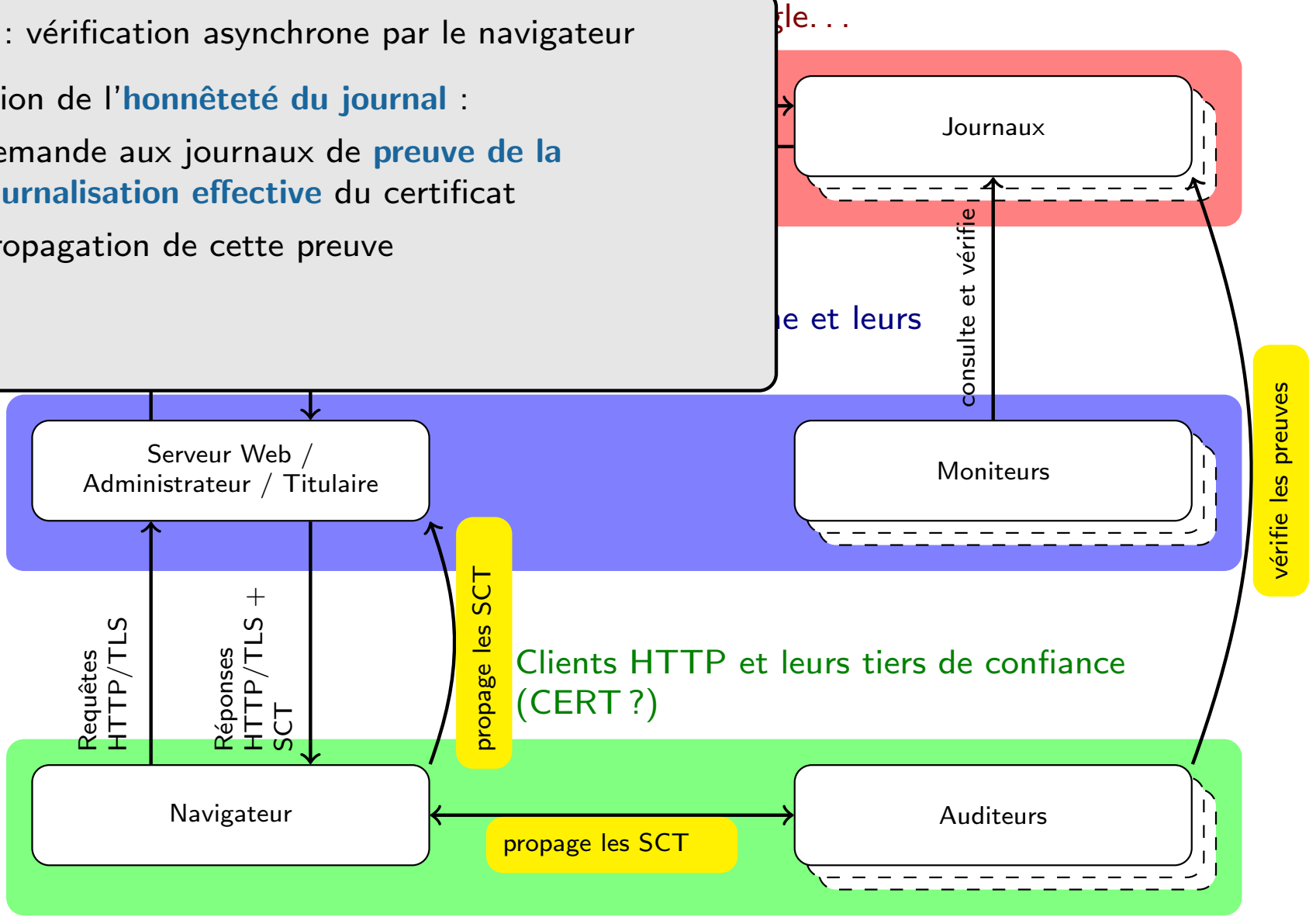
- affichage d'un intersticiel de sécurité
- indicateur visuel

Relations entre les acteurs

Phase 4 : vérification asynchrone par le navigateur

Vérification de l'**honnêteté du journal** :

- demande aux journaux de **preuve de la journalisation effective** du certificat
- propagation de cette preuve



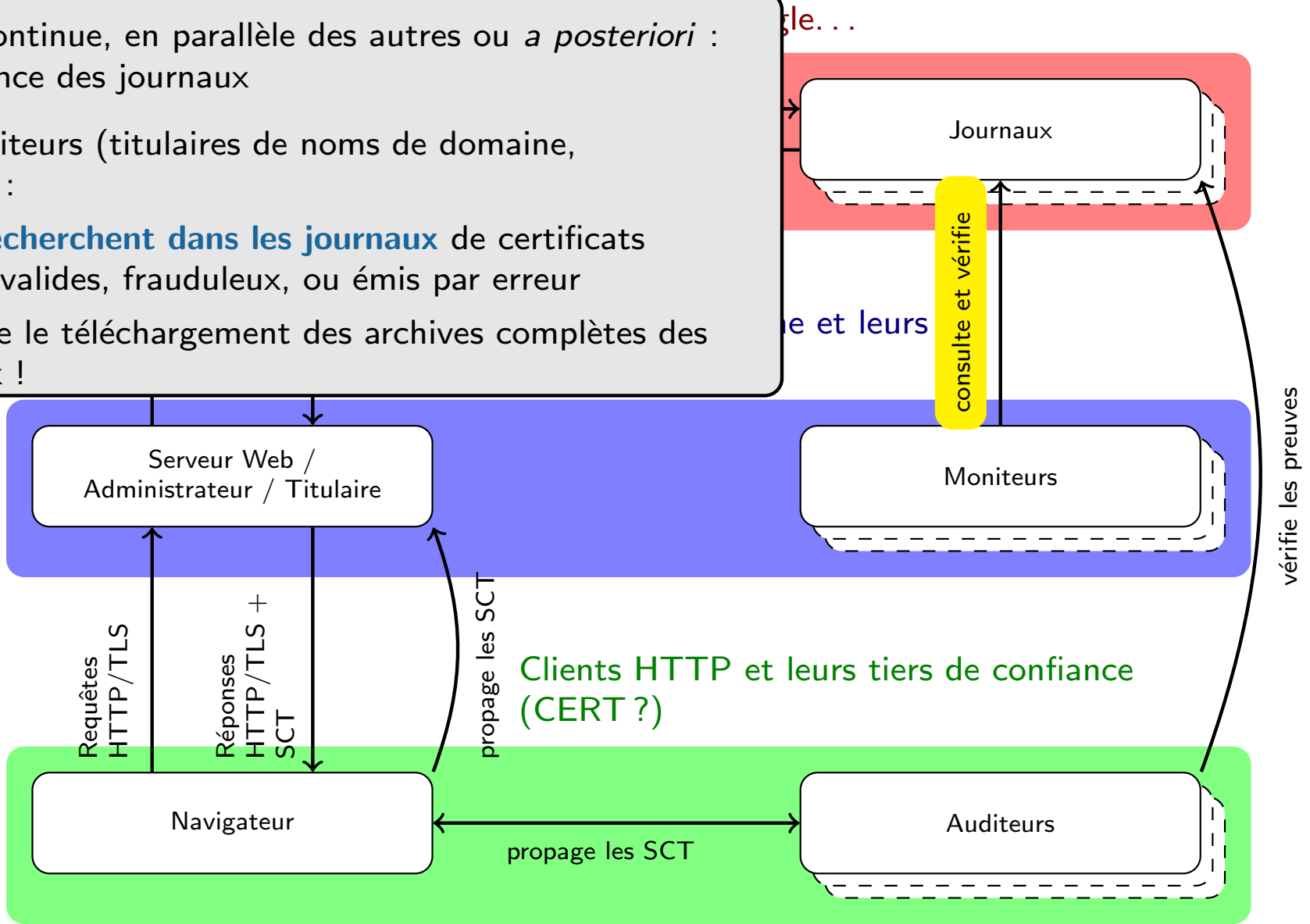
Relations entre les acteurs

Phase continue, en parallèle des autres ou *a posteriori* : surveillance des journaux

Les moniteurs (titulaires de noms de domaine, CERTs) :

- **recherchent dans les journaux** de certificats invalides, frauduleux, ou émis par erreur

Nécessite le téléchargement des archives complètes des journaux !



Certificate Transparency (CT)

en pratique

Implémentation(s) cliente(s)

Clients TLS compatibles à ce jour :

- **Chrom(e|ium)**
- **Firefox 52 Nightly**

Implémentations **partielles** :

- pas de vérification asynchrone (mais remontées par UMA)

Politique CT appliquée par Chrom(e|ium)

Critères :

- nombre d'engagements de journalisation fonction de la durée de validité du certificat
- engagements provenant de journaux **agréés**
- au moins un engagement émis par Google et un autre émis par un tiers

Impact de la politique CT de Chrom(e|ium)

Impact d'un échec de la validation synchrone :

- actuellement :
  - indicateurs visuels (généralement)
  - intersticiel de sécurité (rares cas)
- pour les certificats émis après octobre 2017 :
  - intersticiel de sécurité

Les journaux

Les journaux, en chiffres :

- 12 journaux utilisés dont 5 administrés par Google, 2 par Symantec et 2 par WoSign

Taille du plus gros journal : 48M de certificats ($\approx$ 65Go en Gzip)

Distribution des engagements

Distribution par :

- le certificat (extension X.509)
- l'information de révocation du certificat (extension OCSP)
- le serveur web (extension TLS) :
  - Nginx 1.9+, Apache et HaProxy (trunk)
  - exemple : google.fr, ritter.vg, x-cli.eu
  - Seul moyen ne requérant pas le concours de l'AC

Surveillance des journaux (« moniteurs »)

API en HTTP/JSON :

- permet l'interrogation par relais-proxy

Quelques implémentations *open source* utilisables :

- implémentation de référence par Google
- CertSpotter

Quelques produits en SaaS (gratuits) :

- Digicert Certificate Monitoring
- Comodo CRT.SH

Audit des journaux

Protocole encore non normalisé

- draft-ietf-trans-gossip-03

Création de miroirs

Success stories :

Certificats détectés

avec Certificate Transparency

Incidents détectés avec Certificate Transparency

Exemples d'incidents détectés :

- Symantec : certificats de test
- Facebook : certificats émis par un prestataire
- WoSign/StartSSL : certificats antedatés

Conclusion

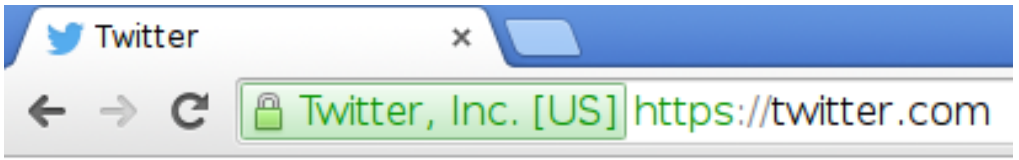
Conclusion : point d'attention №1

Certificate Tranparency (CT) :

- est **déjà déployé**
- contient plusieurs millions de certificats
- est **appliqué** par Chrom(e|ium) et bientôt par Firefox
- sera obligatoire (pour Chrome) à partir d'octobre 2017

Avec Chrom(e|ium) :

- visibilité de la barre verte == CT OK



Conclusion : point d'attention №2

Que retenir de cette présentation ?

- titulaires de noms de domaine et CERTs :
  - **cherchez dans les journaux CT si des certificats ont été émis pour vos noms de domaine et sans votre accord !**

Merci pour votre attention

Bibliographie 1

- Implémentation de référence de CT

  http://github.com/google/certificate-transparency

- Site « Certificate Monitoring » de Digicert

  https://www.digicert.com/certcentral/certificate-monitoring.htm

- Site moniteur de Comodo

  https://crt.sh

- CertSpotter

  https://sslmate.com/certspotter

- Rapport d'incident Symantec

  https://www.symantec.com/connect/sites/default/files/Test_Certificates_Incident_Final_Report_10_13_2015v3b.pdf

Bibliographie 2

- Rapport d'incident Facebook

  https://fr-fr.facebook.com/notes/protect-the-graph/

  early-impacts-of-certificate-transparency/1709731569266987/

- Rapports d'incidents WoSign

  https://wiki.mozilla.org/CA:WoSign_Issues

- Site implémentant un début de protocole de rumeur

  https://ct.grahamedgecombe.com/

- Création de miroirs distribués par Bittorrent

  https://www.x-cli.eu/ct