SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
Rennes 2018

L'Assurance Maladie

CERTIFICATE TRANSPARENCY

ou quand un nouveau standard peut aider votre veille

Christophe Brocas
Thomas Damonneville

Caisse Nationale d'Assurance Maladie – Département Sécurité

AGENDA

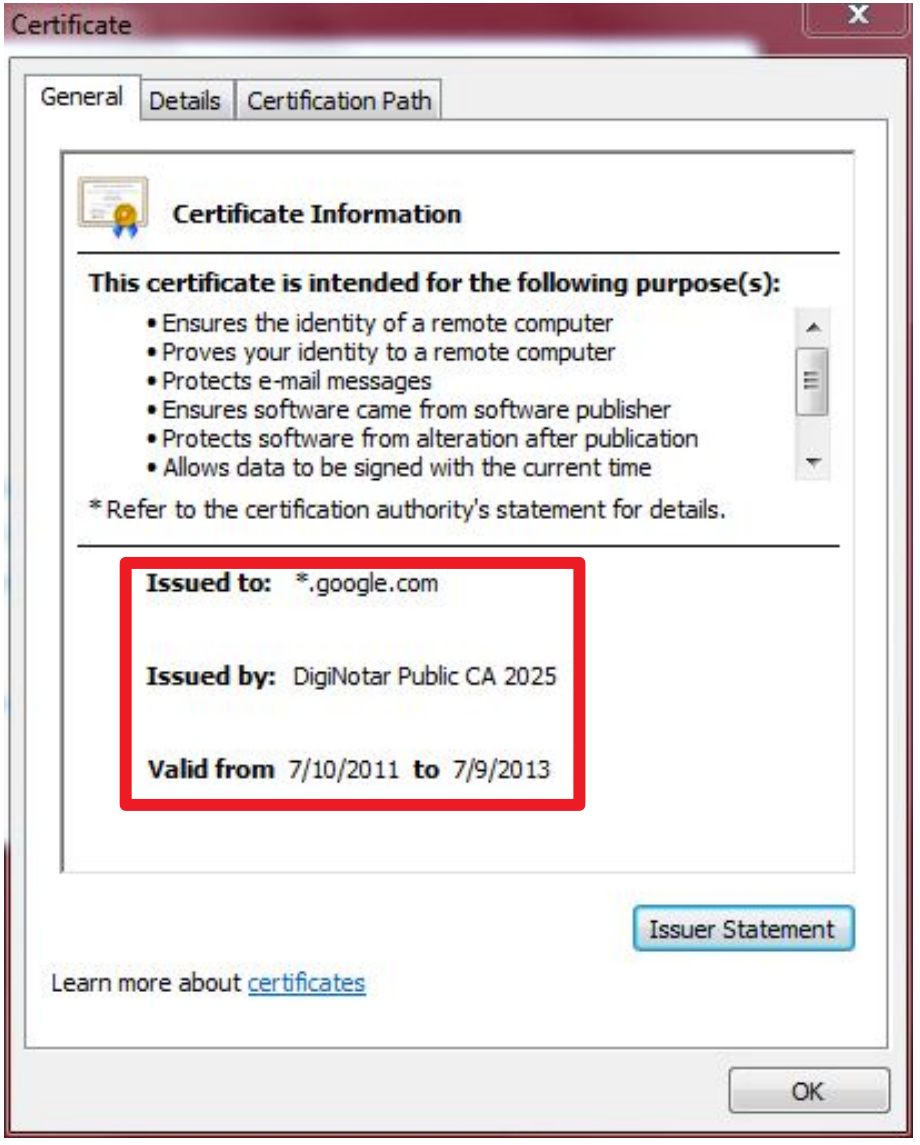
1) le risque / la réponse

2) le fonctionnement de Certificate Transparency

3) ses apports pour votre détection de menaces

→ outils, résultats, limites

LE RISQUE


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• Protects e-mail messages
• Ensures software came from software publisher
• Protects software from alteration after publication
• Allows data to be signed with the current time
* Refer to the certification authority's statement for details.
Issued to: *.google.com
Issued by: DigiNotar Public CA 2025
Valid from 7/10/2011 to 7/9/2013
Issuer Statement
Learn more about certificates
OK

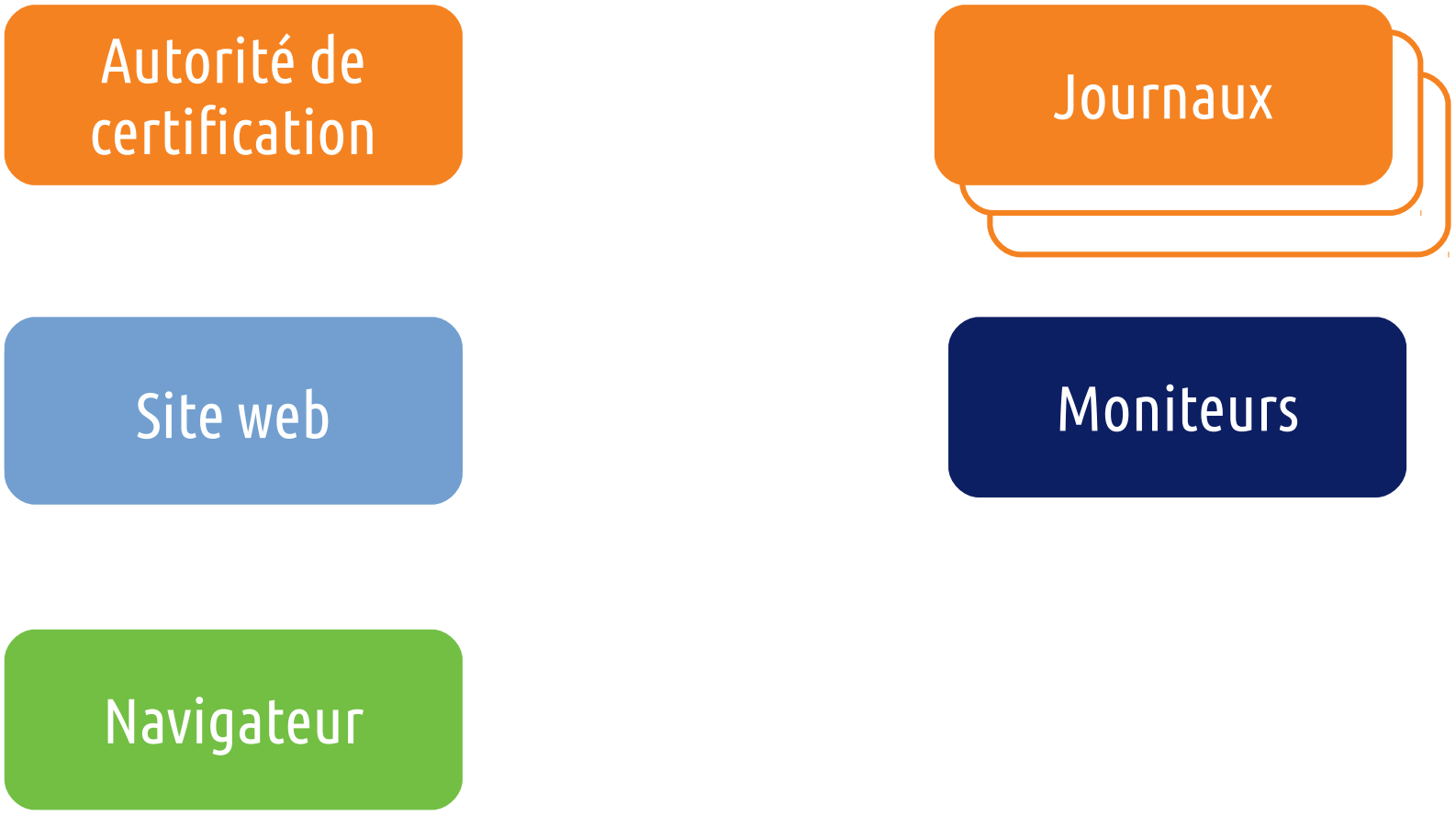
LE RISQUE

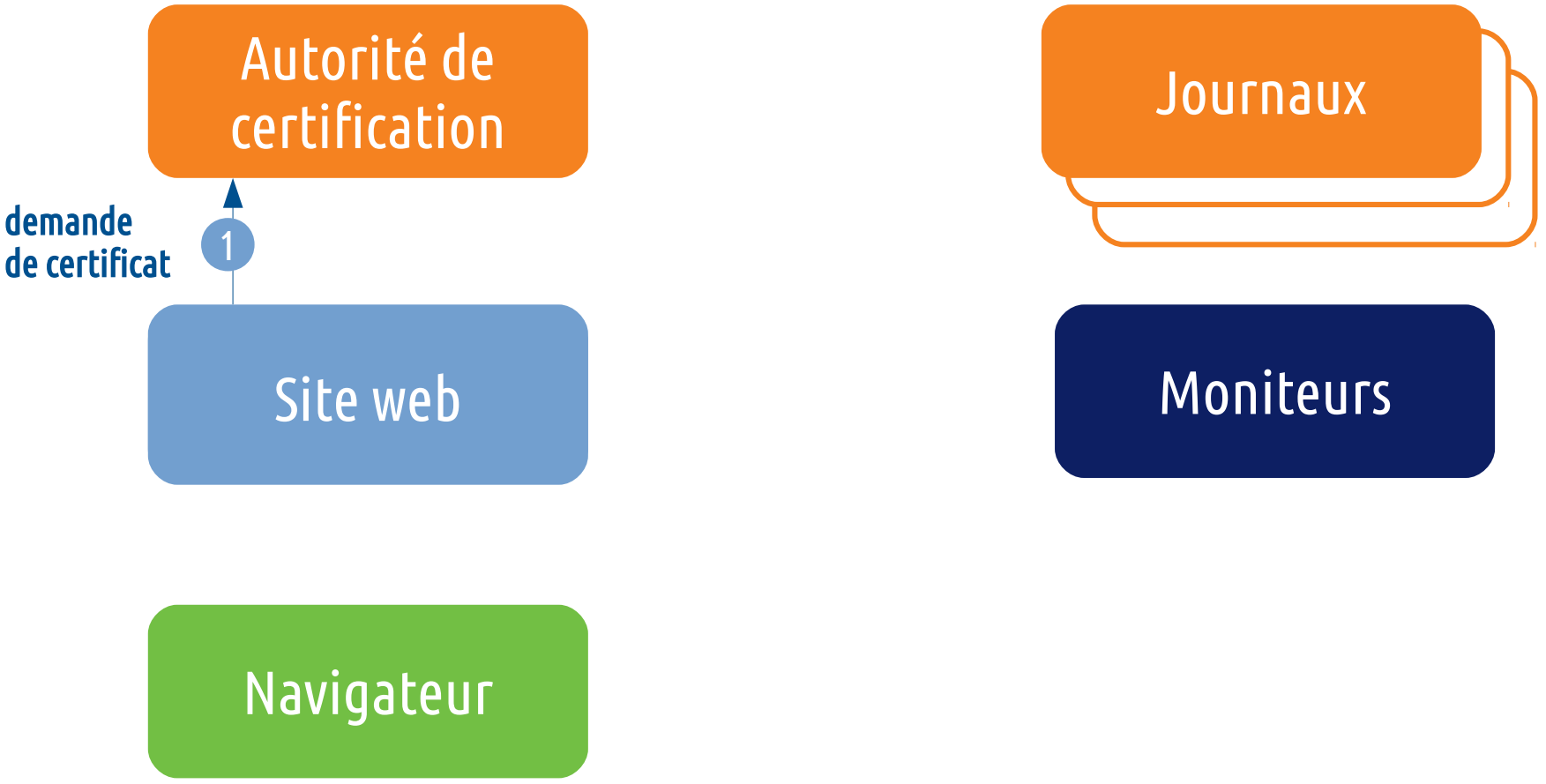
LA REPONSE

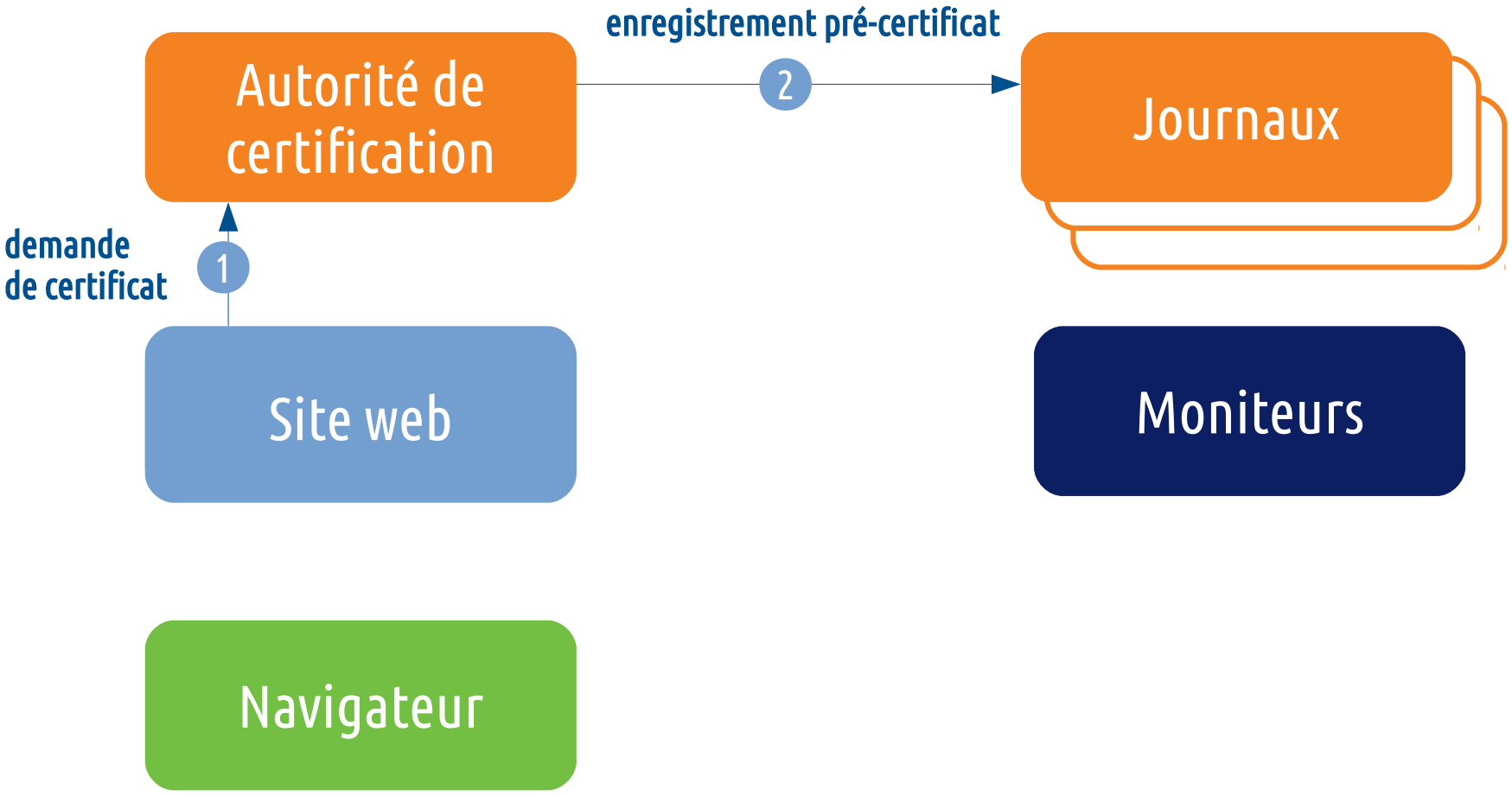
Initiative Google en 2013 (RFC 6962) puis IETF
Toutes les AC doivent consigner tous les certificats publics émis dans des journaux intègres (Merkel Tree) et ouverts.

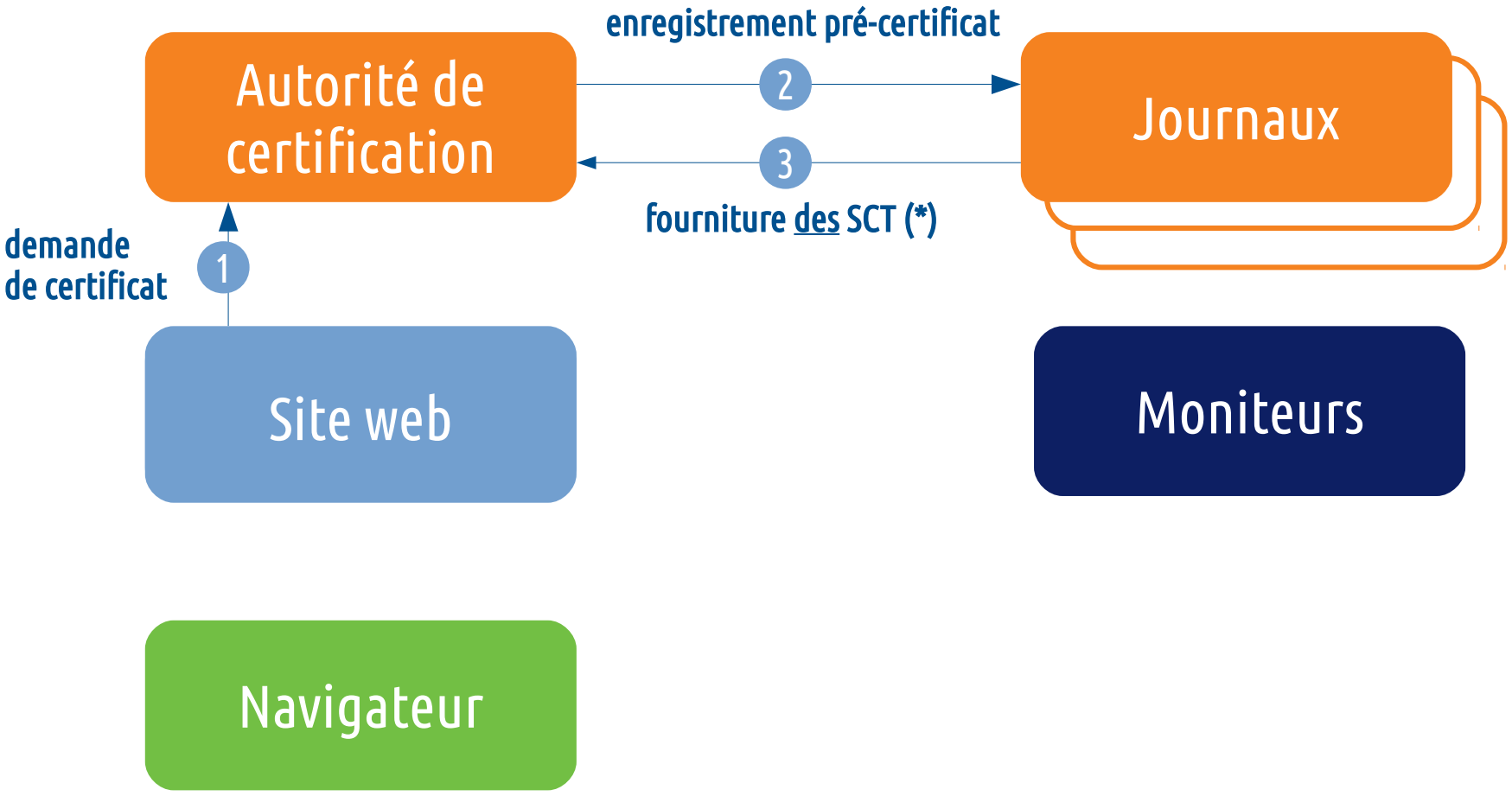
Gain : visibilité sur toutes les émissions de certificats

Échéances :
→ certificats EV : 2015
→ tous les certificats : 30/04/2018
→ fenêtre bloquante dans Chrome 68 : 24/07/2018

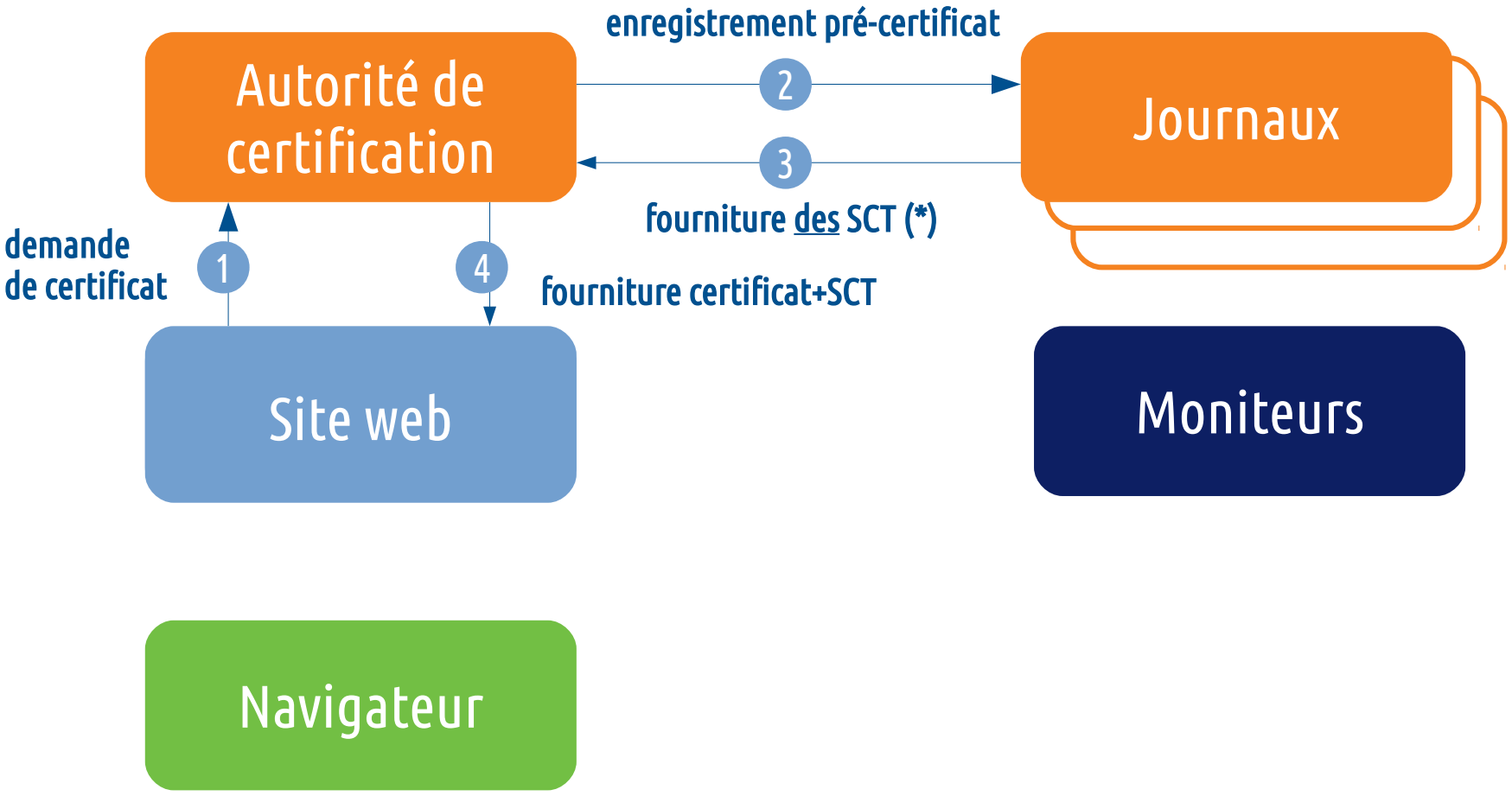

Autorité de certification
Journaux
Site web
Moniteurs
Navigateur


Autorité de certification
demande de certificat
1
Site web
Navigateur
Journaux
Moniteurs

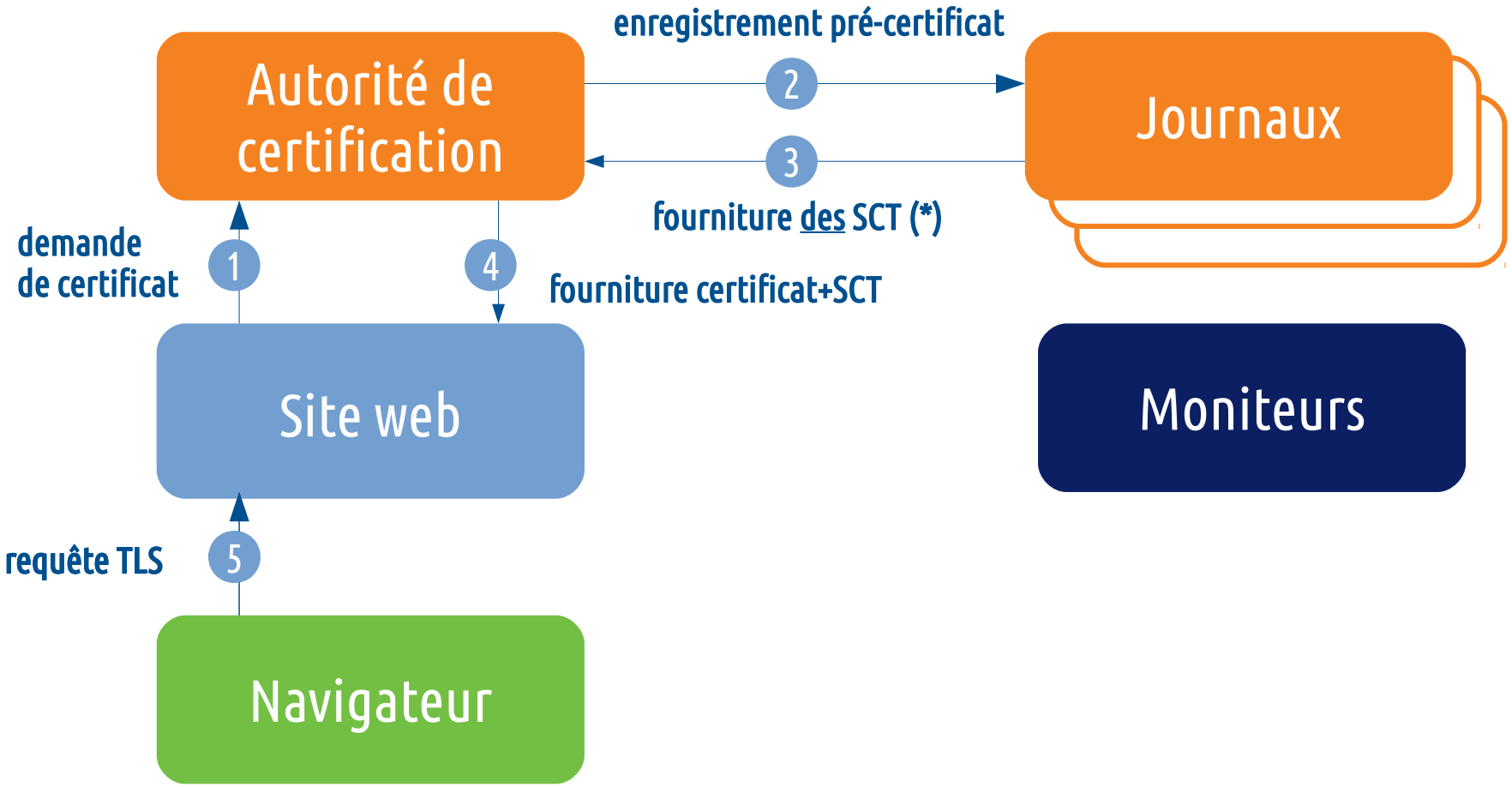

enregistrement pré-certificat
Autorité de certification
2
Journaux
demande de certificat
1
Site web
Moniteurs
Navigateur



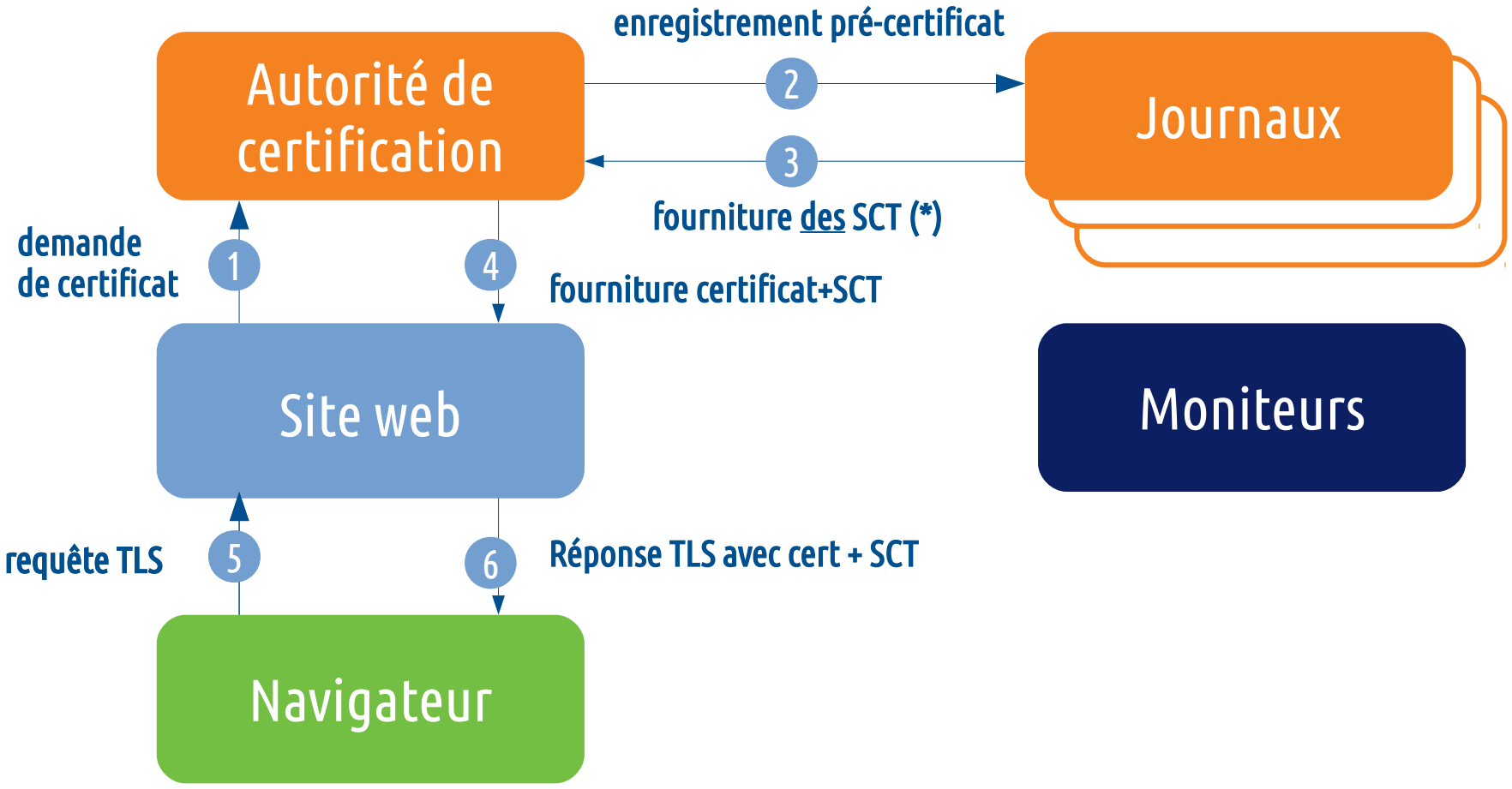
(*) Signed Certificate Timestamp



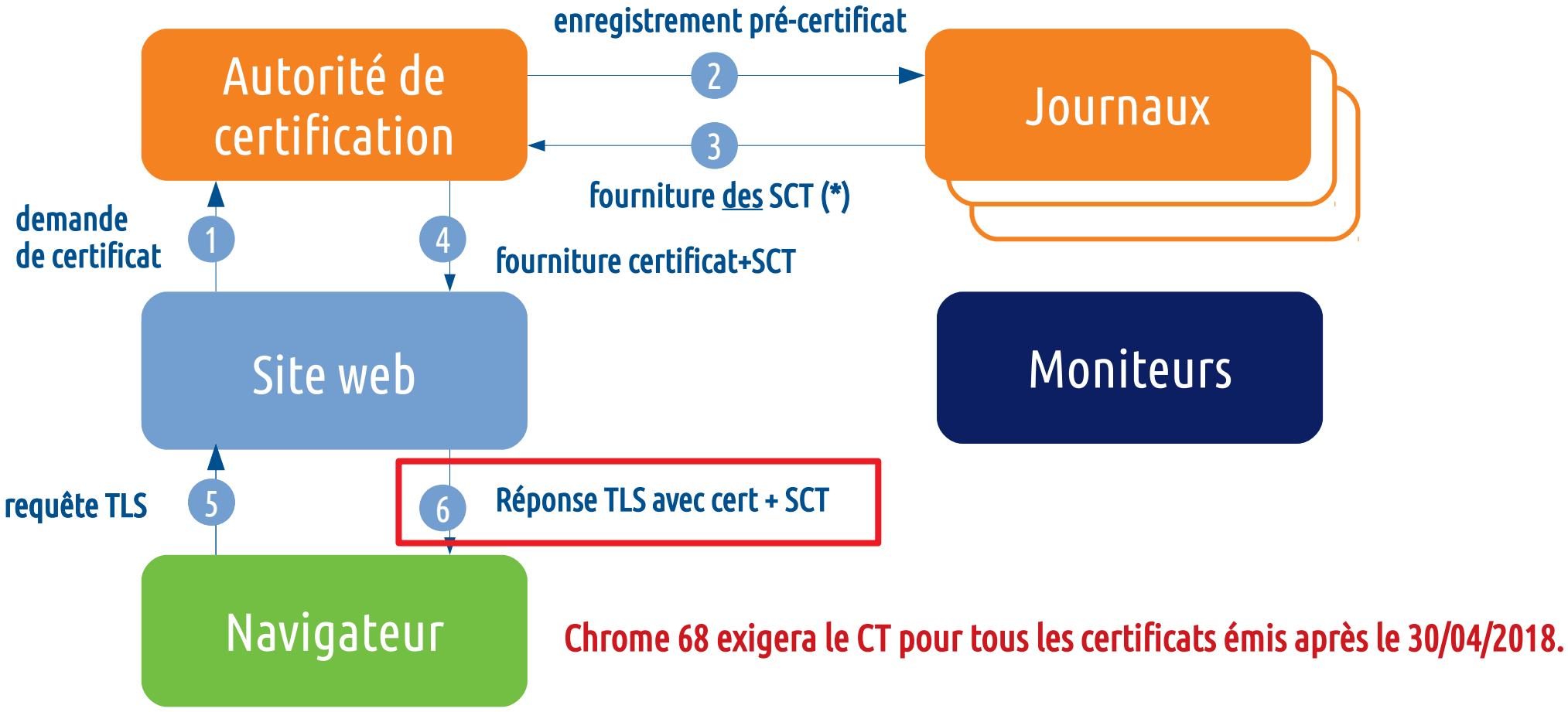
(*) Signed Certificate Timestamp



(*) Signed Certificate Timestamp

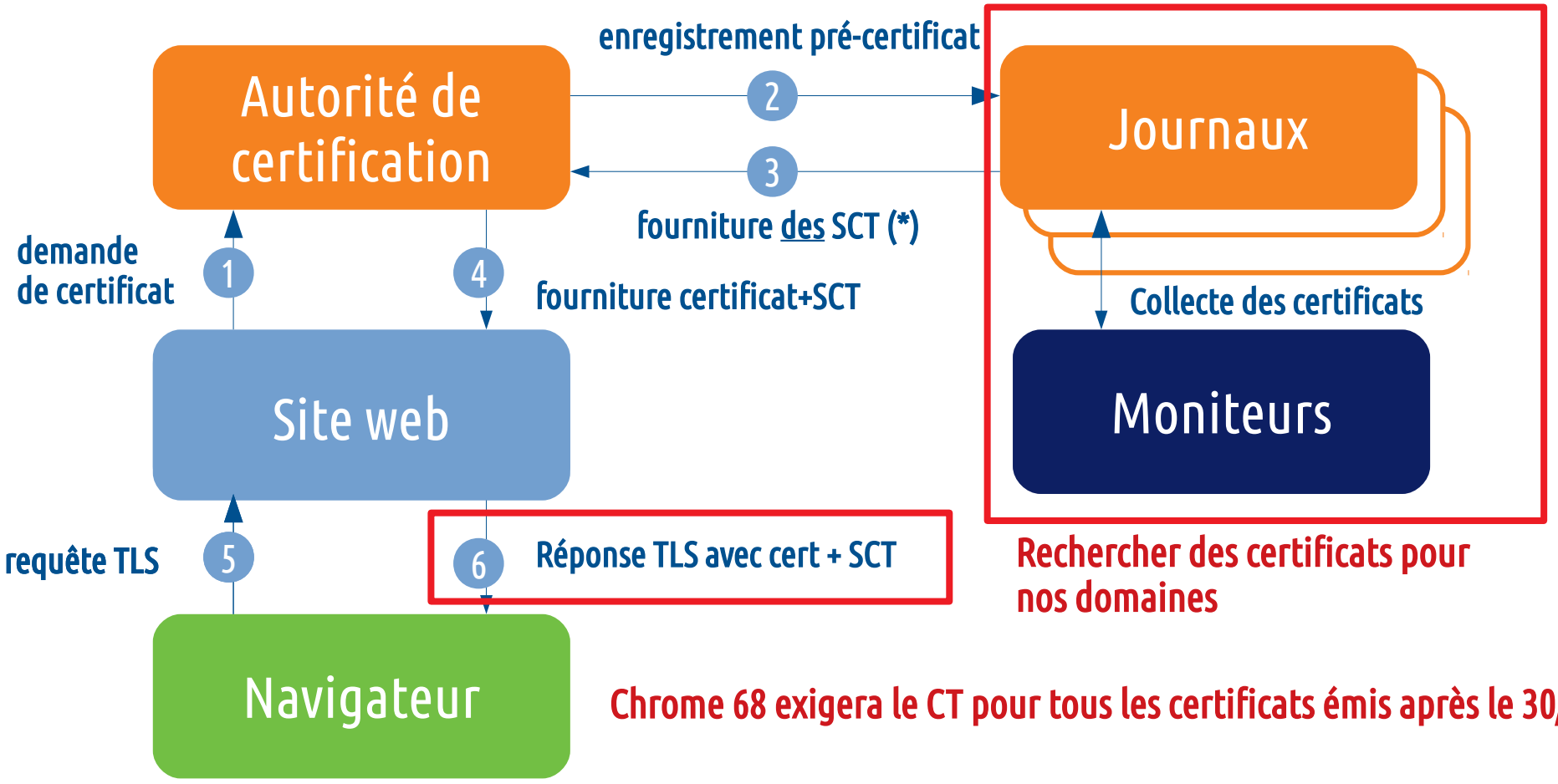


(*) Signed Certificate Timestamp



Chrome 68 exigera le CT pour tous les certificats émis après le 30/04/2018.

(*) Signed Certificate Timestamp



Chrome 68 exigera le CT pour tous les certificats émis après le 30/04/2018.

(*) Signed Certificate Timestamp

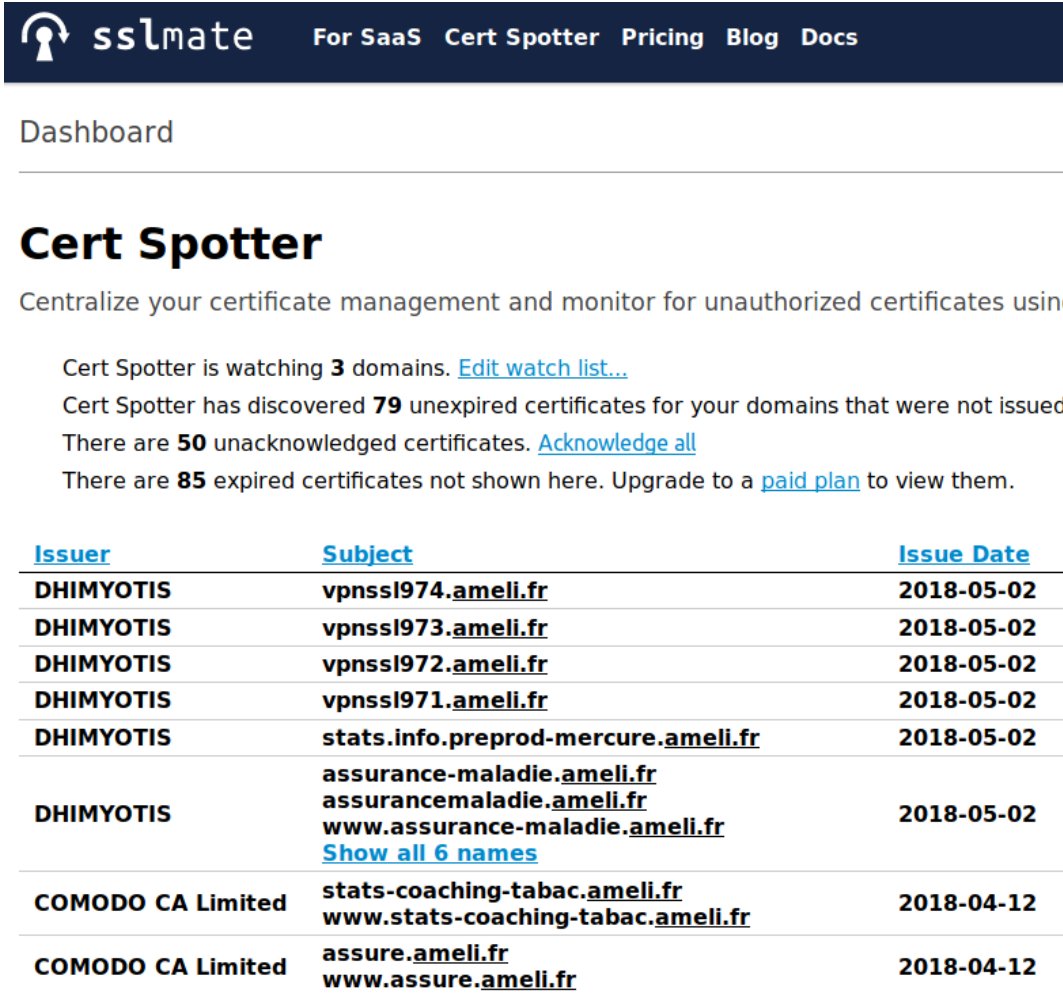
Usage #1 : surveillance de nos domaines

Notre choix actuel :

→ service hébergé

→ notification quotidienne

→ gérée par l'équipe chargée de l'obtention des certificats (efficacité)



sslmate For SaaS Cert Spotter Pricing Blog Docs

Dashboard

Cert Spotter

Centralize your certificate management and monitor for unauthorized certificates usin

Cert Spotter is watching **3** domains. Edit watch list...

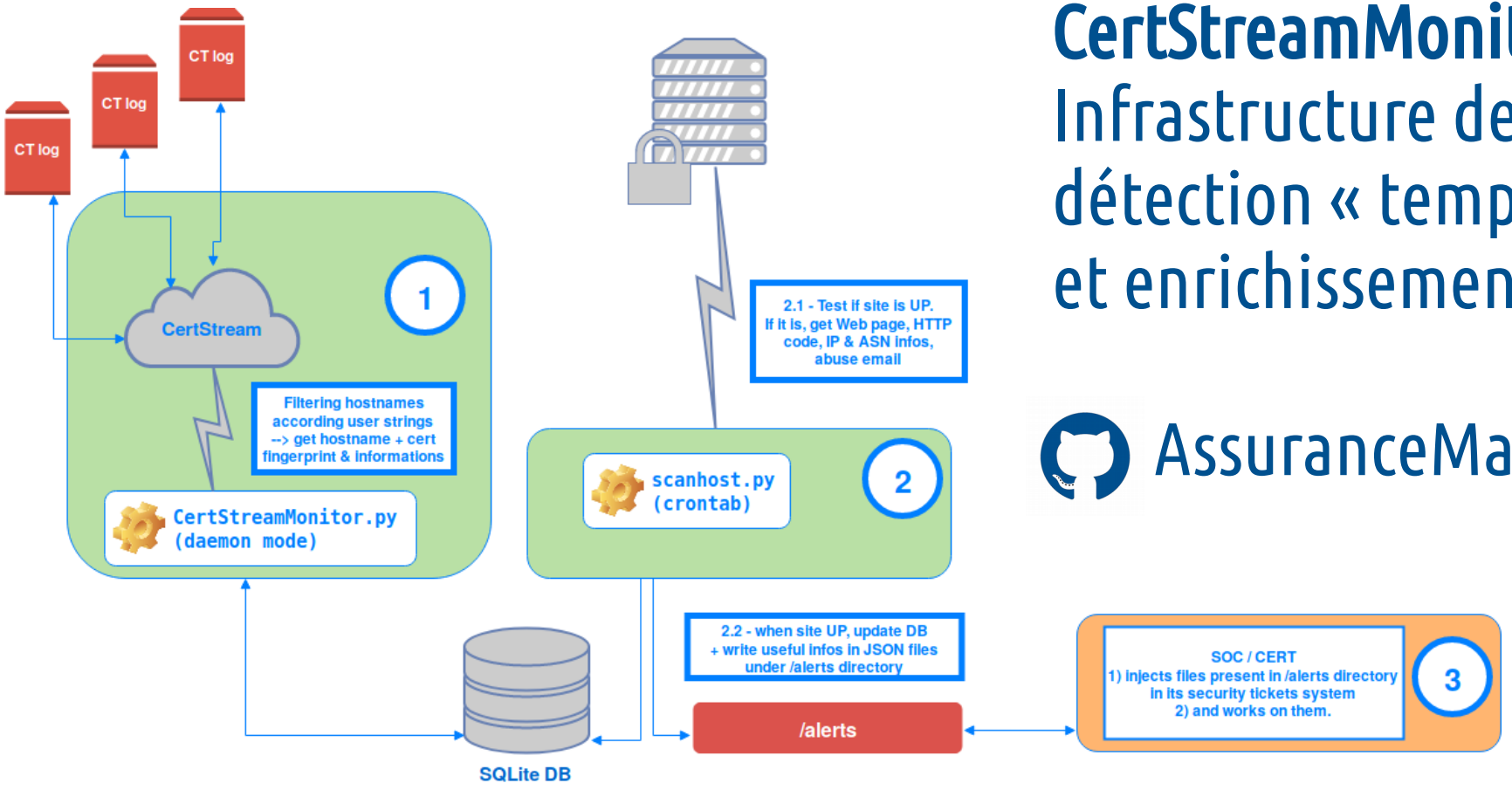
Cert Spotter has discovered **79** unexpired certificates for your domains that were not issued

There are **50** unacknowledged certificates. Acknowledge all

There are **85** expired certificates not shown here. Upgrade to a paid plan to view them.

Issuer	Subject	Issue Date
DHIMYOTIS	vpnssl974.ameli.fr	2018-05-02
DHIMYOTIS	vpnssl973.ameli.fr	2018-05-02
DHIMYOTIS	vpnssl972.ameli.fr	2018-05-02
DHIMYOTIS	vpnssl971.ameli.fr	2018-05-02
DHIMYOTIS	stats.info.preprod-mercure.ameli.fr	2018-05-02
DHIMYOTIS	assurance-maladie.ameli.fr assurancemaladie.ameli.fr www.assurance-maladie.ameli.fr Show all 6 names	2018-05-02
COMODO CA Limited	stats-coaching-tabac.ameli.fr www.stats-coaching-tabac.ameli.fr	2018-04-12
COMODO CA Limited	assure.ameli.fr www.assure.ameli.fr	2018-04-12

Usage #2 : surveillance de domaines «proches»



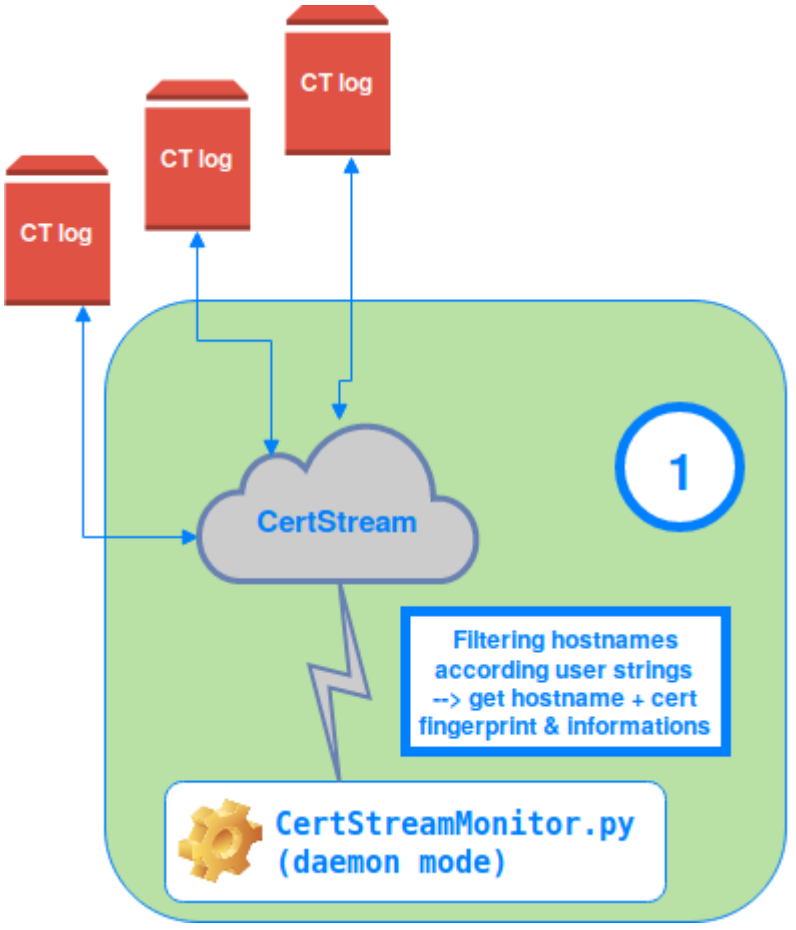
CertStreamMonitor :
Infrastructure de détection « temps-réel » et enrichissement

AssuranceMaladieSec

Usage #2 : surveillance de domaines «proches»

CertStreamMonitor.py

. script sur-mesure
. travaille sur flow consolidé
. détection sur mot-clés
. temps-réel



Usage #2 : surveillance de domaines «proches»

Détection futures campagnes de phishing (CertStreamMonitor.py)

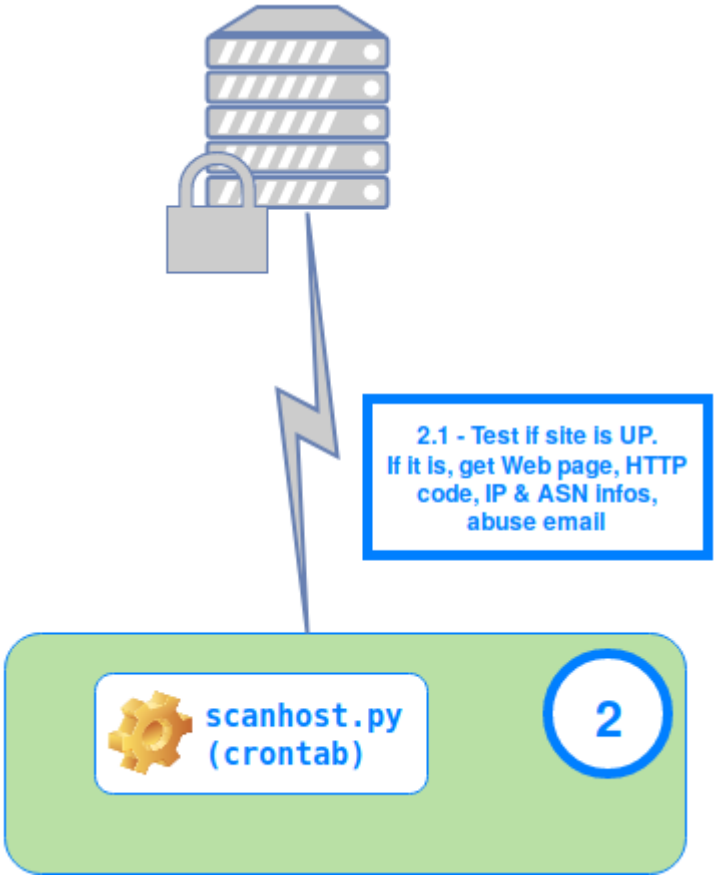
```
assur-frremboursement.cf|2018-05-14T16:40:08|/C=US/CN=Let's Encrypt Authority X3/O=Let's Encrypt
cpanel.remboursement-ameli.online|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursement-ameli.biz|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursement-ameli.org|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursements-ameli.info|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursements-ameli.online|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursements-ameli.org|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursements-ameli.biz|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursements-ameli.xyz|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursements-ameli.us|2018-05-14T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
ameliefashion.amelieaccessories.gr|2018-05-15T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
cpanel.remboursement-ameli.us|2018-05-15T00:00:00|/C=US/CN=cPanel, Inc. Certification Authority/L=Houston/O=cPanel, Inc./ST=TX
remboursement-ameli.online|2018-05-15T11:16:00|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, In
remboursement-ameli.biz|2018-05-15T11:15:42|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc./
remboursements-ameli.us|2018-05-15T11:25:18|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc./
remboursements-ameli.biz|2018-05-15T11:28:20|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc.
remboursement-ameli.us|2018-05-15T11:28:18|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc./O
remboursement-ameli.org|2018-05-15T11:28:16|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc./
remboursements-ameli.org|2018-05-15T11:28:25|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc.
remboursements-ameli.online|2018-05-15T11:28:24|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, I
remboursements-ameli.info|2018-05-15T11:28:22|/C=US/CN=Starfield Secure Certificate Authority - G2/L=Scottsdale/O=Starfield Technologies, Inc
```

Usage #2 : surveillance de domaines «proches»

scanhost.py

si le site est en ligne :

→ enrichissement DB
→ rapport JSON
(ip, AS, email abuse ...)



Usage #2 : surveillance de domaines «proches»

Enrichissement données (scanhost.py)

```
Test all domains in DB for Internet Presence:
**********************************************
11:19:58 - ERROR -   https://remboursements-ameli.info - Connection error
11:20:00 - SUCCESS - HTTP 200 - remboursement.ameli.amameli.com
Creating ./alerts/remboursement.ameli.amameli.com.json : {'hostname': 'remboursement.ameli.amameli.com', 'htt
p_code': 200, 'cert_serial_number': 'DE:9F:E8:81:0D:23:6D:C3:8D:E3:6B:33:86:BD:4A:9E:7E:4F:5E:07', 'webpage_t
itle': 'Account Suspended', 'ip_addr': '72.18.132.239', 'asn': '30475', 'asn_cidr': '72.18.128.0/19', 'asn_co
untry_code': 'US', 'asn_description': 'WEHOSTWEBSITES-COM - Handy Networks, LLC, US', 'asn_abuse_email': 'abu
se@wehostwebsites.com'}
11:20:01 - ERROR -   https://assurance-maladie.cf - Connection error
11:20:04 - SUCCESS - HTTP 200 - assure.ameli.fr.eskandiromagic.info
Creating ./alerts/assure.ameli.fr.eskandiromagic.info.json : {'hostname': 'assure.ameli.fr.eskandiromagic.inf
o', 'http_code': 200, 'cert_serial_number': '53:F6:23:A0:16:11:5D:47:39:1D:C1:07:54:0C:4F:01:02:D8:C3:DD', 'w
ebpage_title': 'Compte ameli - mon espace personnel - Connexion &agrave; mon compte', 'ip_addr': '162.213.123
.155', 'asn': '40244', 'asn_cidr': '162.213.120.0/22', 'asn_country_code': 'US', 'asn_description': 'TURNKEY-
INTERNET - Turnkey Internet Inc., US', 'asn_abuse_email': 'abuse@turnkeyinternet.net'}
```

Usage #2 : surveillance de domaines «proches»

Rapport JSON (scanhost.py)

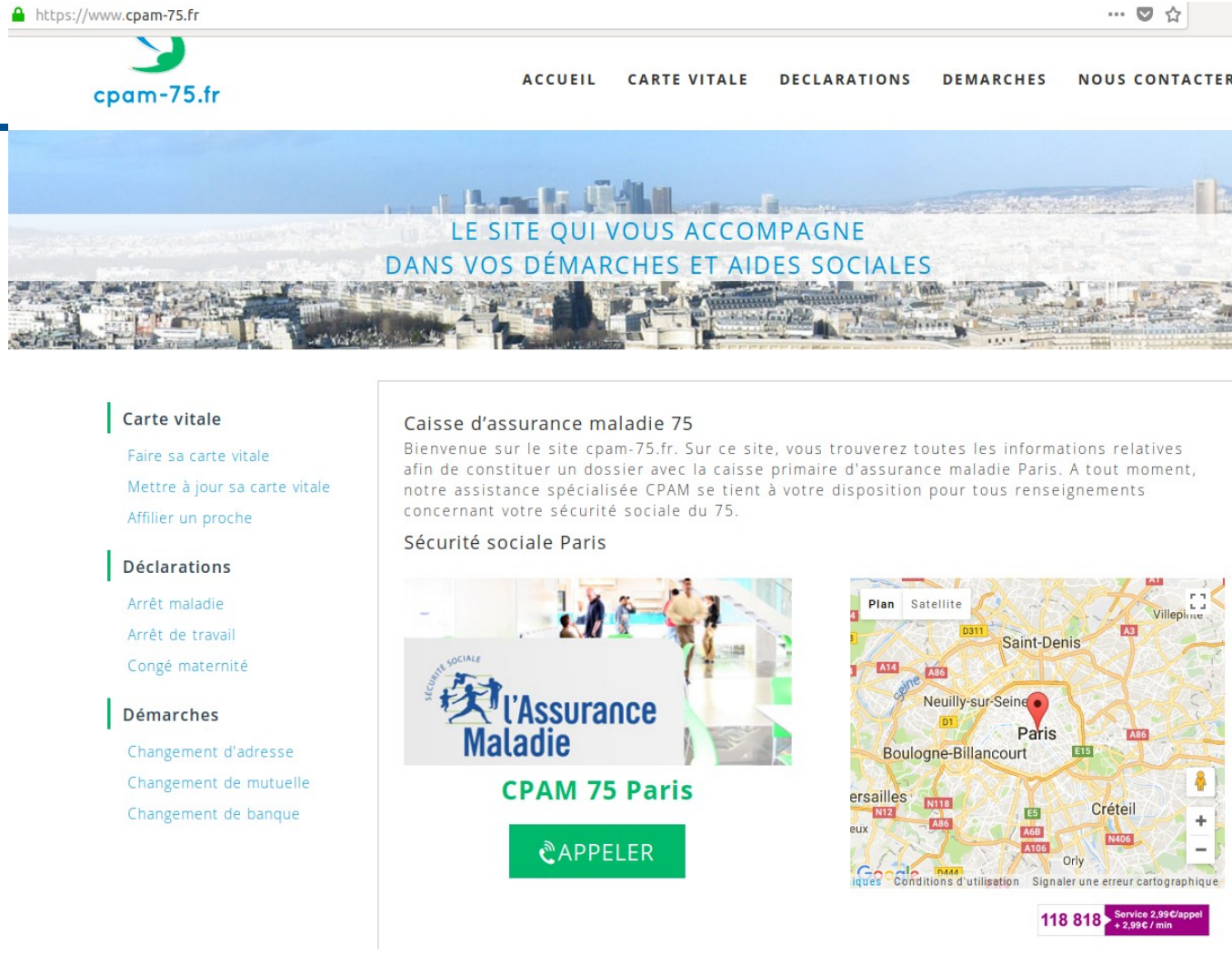

```
{
    "hostname": "assure.ameli.fr.eskandiromagic.info",
    "http_code": 200,
    "cert_serial_number": "53:F6:23:A0:16:11:5D:47:39:1D:C1:07:54:0C:4F:01:02:D8:C3:DD",
    "webpage_title": "Compte ameli - mon espace personnel - Connexion &agrave; mon compte",
    "ip_addr": "162.213.123.155",
    "asn": "40244",
    "asn_cidr": "162.213.120.0/22",
    "asn_country_code": "US",
    "asn_description": "TURNKEY-INTERNET - Turnkey Internet Inc., US",
    "asn_abuse_email": "abuse@turnkeyinternet.net"
}
```

Résultats

Exemple #1 : abus de nos utilisateurs

cpam-{78,75,13,...}.fr

→ service abusant potentiellement nos assurés (n° surtaxés, données personnelles)

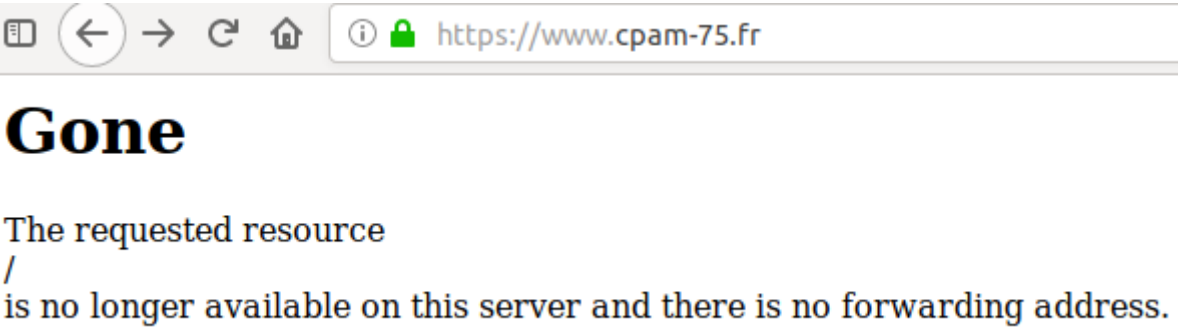


Résultats

Exemple #1 : abus de nos utilisateurs

cpam-{78,75,13,...}.fr

→ service abusant potentiellement nos assurés (n° surtaxés, données personnelles)
→ inactivation du service



Résultats

Exemple #2 : maitrise du SI

[redacted]li.fr

. service légitime
. préconisations non suivies :
(nom de domaine, hébergement etc)

Limites de l'approche

- TLS, pas HTTP - détection uniquement des hostnames protégés par TLS
- RegExp - si le hostname n'a pas de chaines de caractères proches de vos mots clefs → pas de détection.
- Confiance - le volume de données engendré oblige à passer par des intermédiaires (moniteurs). A qui peut-on faire confiance ?

Conclusion

~~aveugle~~
vision à l'échelle d'Internet

efficacité
informé avant la mise en ligne de l'attaque

low cost
les outils et services sont à disposition.

Merci !

Des questions ?

https://github.com/AssuranceMaladieSec

christophe.brocas@assurance-maladie.fr
thomas.damonneville@assurance-maladie.fr

@cbrocas | @o0tAd0o