

---

---

**POLITICA DE CERTIFICARE  
A  
AUTORITĂȚII DE CERTIFICARE A  
SERVICIULUI DE TELECOMUNICAȚII SPECIALE  
(STS)**

**-STS PC-**

---

---

## CUPRINS

<b>INTRODUCERE.....</b>	<b>3</b>
<b>CERTIFICATE.....</b>	<b>3</b>
AUTORITATEA DE CERTIFICARE STS CLASA 1 .....	4
AUTORITATEA DE CERTIFICARE STS CLASA 2 .....	4
AUTORITATEA DE CERTIFICARE STS CLASA 3 .....	4
AUTORITATEA DE CERTIFICARE STS CLASA 4 .....	5
<b>ACCEPTAREA CERTIFICATULUI.....</b>	<b>5</b>
<b>SERVICII DE CERTIFICARE .....</b>	<b>6</b>
<b>SERVICIUL DE MARCĂ TEMPORALĂ.....</b>	<b>6</b>
<b>SERVICIUL DE VALIDARE AL CERTIFICATELOR DIGITALE .....</b>	<b>6</b>
<b>TERTĂ PARTE .....</b>	<b>7</b>
<b>ABONATUL.....</b>	<b>7</b>
<b>ACTUALIZAREA POLITICII DE CERTIFICARE .....</b>	<b>7</b>

## **Introducere**

Infrastructura cu chei publice a S.T.S. are scopul de a oferi soluții (produse și servicii) de securitate a rețelelor de calculatoare și a aplicațiilor informatice destinate nevoilor proprii ale S.T.S. precum și ale beneficiarilor legali.

Prezentul document reprezintă Politica de Certificare aplicabilă Infrastructurii cu chei publice a STS. Politica de Certificate a S.T.S. (PC) reglementează folosirea certificatelor în cadrul diferitelor structuri ale S.T.S. cât și pentru beneficiarii legali; ea reprezintă politica unitară sub care operează toate AC-urile din cadrul STS. PC STS nu definește o anume implementare a unui PKI și nici nu definește politica de certificare pentru AC-uri operate de către entități externe, în numele STS.

## **Certificate**

Certificatele identifică persoana specificată în certificat și asociază acelei persoane o anumită pereche de chei publică/privată.

Acest document definește modul de creare și gestiune a certificatelor cu chei publice X.509 Versiunea 3, pentru utilizarea lor în aplicații ce solicită comunicarea între sisteme bazate pe calculatoare conectate în rețea. Astfel de aplicații includ, dar nu se limitează la:

- poșta electronică,
- transmiterea informațiilor secrete și nesecrete,
- semnarea formularelor electronice,
- semnarea documentelor electronice și a contractelor și
- autentificarea componentelor de infrastructură cum sunt serverele de web, firewall-uri, rutere și directoare.

Tipurile de rețele în care se utilizează certificatele digitale sunt :

- rețele neprotejate (Internet)
- rețeaua internă a S.T.S. (Intranet STS)
- rețele protejate ale S.T.S.

Autoritatea de Certificare a Serviciului de Telecomunicații Speciale (AC-STS) implementează patru nivele de încredere pentru certificatele pe care le emite, în funcție de:

- categoria de informație care poate fi manipulată utilizând respectivele certificate;
- tipurile de aplicații ce pot fi utilizate cu respectivele certificate;
- tipul entității pentru care se emite certificatul (persoană sau dispozitiv);

- modalitatea de păstrare a cheii private a utilizatorului – pe token (smartcard) sau în fișier.

### **Autoritatea de Certificare STS Clasa 1**

CertIFICATELE emise cu acest nivel de încredere sunt destinate numai persoanelor fizice. Ele pot fi folosite pentru protejarea informațiilor publice, a celor neclasificate nedestinate publicității și a celor clasificate cu nivelul maxim secret de serviciu, care sunt vehiculate în toate tipurile de rețele (publice, Internet, Intranet STS, clasificate), în toate tipurile de aplicații care sunt compatibile cu standardul ITU-T X.509. Cheia privată se emite pe token sau smartcard.

Politica de emiteră a certificatelor cu acest nivel de încredere are următorul identificator: 1.3.6.1.4.1.20625.1.1.1

Valabilitatea unui certificat emis sub această clasă este de un an calendaristic.

### **Autoritatea de Certificare STS Clasa 2**

CertIFICATELE emise cu acest nivel de încredere sunt destinate numai persoanelor fizice. Ele pot fi folosite pentru protejarea informațiilor publice, a celor neclasificate nedestinate publicității, a celor clasificate cu nivelul maxim secret de serviciu precum și pentru protejarea informațiilor secrete de stat cu nivele de secretizare corespunzătoare nivelului de certificare de securitate al aplicațiilor compatibile ITU-T X.509, stabilit în conformitate cu cerințele legislației naționale privind protecția informațiilor clasificate.

CertIFICATELE STS Clasa 2 pot fi utilizate în toate tipurile de rețele (publice, Internet, Intranet STS, clasificate) și în toate tipurile de aplicații care sunt compatibile cu standardul ITU-T X.509. Cheia privată se emite pe token sau smartcard.

Politica de emiteră a certificatelor din această clasă are următorul identificator: 1.3.6.1.4.1.20625.1.1.2

Valabilitatea unui certificat emis sub această clasă este de un an calendaristic.

### **Autoritatea de Certificare STS Clasa 3**

CertIFICATELE emise cu acest nivel de încredere sunt destinate numai dispozitivelor și serverelor. Ele pot fi folosite pentru protejarea informațiilor publice, a celor neclasificate nedestinate publicității și a celor clasificate cu nivelul maxim secret de serviciu, care sunt vehiculate în toate tipurile de rețele (publice, Internet, Intranet STS, clasificate), în toate

tipurile de aplicații care sunt compatibile cu standardul ITU-T X.509. Politica de emitere a certificatelor din această clasă are următorul identificator: 1.3.6.1.4.1.20625.1.1.3

Valabilitatea unui certificat emis sub această clasă este de un an calendaristic.

### **Autoritatea de Certificare STS Clasa 4**

CertIFICATELE emise cu acest nivel de încredere sunt destinate numai dispozitivelor și serverelor. Ele pot fi folosite pentru protejarea informațiilor publice, a celor neclasificate nedestinate publicității, a celor clasificate cu nivelul maxim secret de serviciu precum și pentru protejarea informațiilor secrete de stat cu nivele de secretizare corespunzătoare nivelului de certificare de securitate al aplicațiilor compatibile ITU-T X.509, stabilit în conformitate cu cerințele legislației naționale privind protecția informațiilor clasificate.

CertIFICATELE STS Clasa 4 pot fi utilizate în toate tipurile de rețele (publice, Internet, Intranet STS, clasificate) și în toate tipurile de aplicații care sunt compatibile cu standardul ITU-T X.509.

Politica de emitere a certificatelor din această clasă are următorul identificator: 1.3.6.1.4.1.20625.1.1.4

Valabilitatea unui certificat emis sub această clasă este de un an calendaristic.

### **Acceptarea certificatului**

Acceptarea certificatului de către utilizator presupune că acesta este de acord cu următoarele:

- fiecare semnătură digitală creată utilizând cheia privată corespunzătoare cheii publice listată în certificat este semnătura digitală a utilizatorului și certificatul acceptat este operațional (nu este expirat, suspendat sau revocat) la data și ora la care a fost creată semnătura digitală;
- nici o persoană neautorizată nu a avut acces la cheia privată a utilizatorului;
- informațiile conținute în certificat sunt adevărate;
- certificatul poate fi utilizat numai în scopuri autorizate de STS;
- abonatul, în calitatea sa de utilizator final, nu poate utiliza cheia sa privată corespunzătoare cheii publice listată în certificat pentru semnarea altor certificate sau liste de revocare, decât în cazurile în care acest lucru a fost prevăzut expres în contractul semnat cu autoritatea sa de certificare.

Prin acceptarea certificatului, abonatul (utilizatorul) își asumă responsabilitatea controlului cheii sale private și luarea unor precauții pentru a preveni pierderea, dezvăluirea, modificarea sau utilizarea neautorizată a acesteia.

## **Servicii de certificare**

Înregistrarea cererii de certificat pentru un utilizator se realizează printr-un număr de pași descriși în cadrul Codului de Practici și Proceduri al Serviciului de Telecomunicații Speciale (CPP):

- Stabilirea și înregistrarea utilizatorului;
- Obținerea unei perechi de chei, publică și privată;
- Stabilirea faptului că cheia publică are ca pereche cheia privată deținută de utilizator;
- Furnizarea unor puncte de contact pentru verificarea tuturor rolurilor sau autorizațiilor cerute de abonat.

Un abonat își poate reînnoi un certificat și acest proces este descris în Codul de Practici și Proceduri al Serviciului de Telecomunicații Speciale.

Certificatul unui abonat poate fi revocat. Condițiile în care se revocă un certificat se referă la compromiterea cheii utilizatorului, modificarea datelor de identificare a utilizatorului precum și alte circumstanțe ce sunt prezentate în CPP. Certificatele revocate sunt plasate în listele de certificate revocate (LCR) până la expirarea lor.

Pentru revocarea unui certificat, utilizatorul trebuie să urmeze anumite proceduri care sunt descrise în cadrul CPP.

## **Serviciul de marcă temporală**

STS oferă serviciul de marcă temporală în scopul garantării existenței documentelor electronice la un moment dat. Mărcile temporale sunt emise cu o acuratețe de 1 secundă.

Identificatorul politicii autorității de certificare TSA este inclus în fiecare token de marcă temporală.

## **Serviciul de validare al certificatelor digitale**

STS oferă serviciul de validare al certificatelor digitale bazat pe protocolul OCSP (On Line Certificate Status Protocol), ca o alternativă la utilizarea listelor de certificate revocate. Prin acest serviciu, STS garantează furnizarea corectă a stării de revocare a unui certificat digital emis de AC-STS.

## **Terță parte**

Un terț este entitatea care, folosind certificatul altuia pentru a verifica integritatea unui mesaj semnat digital, pentru a identifica pe cel care a creat mesajul sau pentru a stabili o comunicare confidențială cu posesorul certificatului, se încrede în validitatea legăturii nume utilizator – cheie publică.

O terță parte este obligată să verifice semnătura digitală asociată cu un document pe care l-a primit. În procesul de verificare a unei semnături digitale create pe baza unui certificat emis de AC-STS, trebuie să utilizeze proceduri și resurse ale STS.

## **Abonatul**

Abonatul este entitatea al cărei nume apare ca subiect într-un certificat și care revendică folosirea cheii sale în concordanță cu politica de certificare.

Abonatul are obligația de a-și proteja permanent cheia privată, în concordanță cu CPP. El trebuie să semnaleze despre următoarele evenimente care pot apărea în timpul perioadei de valabilitate a certificatului:

- cheia lui privată a fost compromisă, furată sau pierdută;
- a fost afectat controlul asupra cheii private, prin pierderea sau compromiterea datelor de activare (ex. PIN);
- neconcordanțe sau modificări în conținutul certificatului.

Abonatul va respecta toate termenele, condițiile și restricțiile impuse asupra utilizării cheilor private și a certificatelor asociate.

El va folosi certificate furnizate de S.T.S. numai pentru tranzacții legate de activitățile S.T.S.

## **Actualizarea politicii de certificare**

AC-STS revizuieste această politică periodic, cel puțin o dată în fiecare an. Erorile, update-urile sau sugestiile de schimbare ale acestui document vor fi comunicate persoanelor de legătură desemnate pentru acest scop. Fiecare comunicare va include o descriere a schimbării solicitate, o justificare a ei și informații de contact pentru persoana care a cerut schimbarea.

Toate schimbările care sunt în studiul AC-STS, vor fi diseminate părților interesate pentru o perioadă de cel puțin două luni.