



# Profilul certificatului calificat al Root CA

Profiluri și parametri pentru certificatul Root CA

Prezentul document definește profilul certificatului calificat utilizat de Simplifi, în calitate de Furnizor de Servicii de Încredere Calificat (QTSP). Acesta descrie structura și

parametrii specifici pentru certificatul Autorității de Certificare Rădăcină (Root CA).

## Informații despre document

|                         |                                              |
|-------------------------|----------------------------------------------|
| Versiune                | 1.0                                          |
| Data versiunii          | 1 septembrie 2025                            |
| Aprobat de              | CEO                                          |
| Responsabil de document | Manager Servicii de Încredere                |
| Nume document           | Profilul Certificatului Calificat al Root CA |
| OID Document            | 1.3.6.1.4.1.63578.1.5.3                      |
| Clasificare Document    | Public                                       |

## Istoric document

| Versiune | Data intrării în vigoare | Motiv              | Autor                         |
|----------|--------------------------|--------------------|-------------------------------|
| V 1.0    | 2025-09-01               | Publicare inițială | Manager Servicii de Încredere |

## Istoric aprobare

| Versiune | Data aprobare | Aprobat de |
|----------|---------------|------------|
| V 1.0    | 2025-09-01    | CEO        |

## Istoric distribuire

| Versiune | Data distribuire | Distribuit de         |
|----------|------------------|-----------------------|
| V 1.0    | 2025-09-01       | Trust Service Manager |

## Cuprins

|                                                                       |          |
|-----------------------------------------------------------------------|----------|
| Informații despre document.....                                       | 2        |
| Istoric document .....                                                | 2        |
| Istoric aprobare .....                                                | 2        |
| Istoric distribuire.....                                              | 2        |
| <b>1. Introducere .....</b>                                           | <b>4</b> |
| <b>2. Profil tehnic al certificatului.....</b>                        | <b>4</b> |
| <b>3. Structura certificatului .....</b>                              | <b>4</b> |
| 3.1. Certificatul Autorității de Certificare Rădăcină (Root CA) ..... | 4        |
| 3.2. Profil CRL .....                                                 | 5        |

## 1. Introducere

Prezentul document descrie profilul certificatului pentru Autoritatea de Certificare Rădăcină (Root CA) și profilul asociat al Listei de Revocare a Certificatelor (CRL).

## 2. Profil tehnic al certificatului

Certificatul este generat în conformitate cu standardele X.509 versiunea 3, IETF RFC 5280, ETSI EN 319 412-2 și ETSI EN 319 411-2.

## 3. Structura certificatului

### 3.1. Certificatul Autorității de Certificare Rădăcină (Root CA)

| Profilul Certificatului Root CA         |             |                        |                                                                                                                                                                                 |
|-----------------------------------------|-------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Câmp                                    | Obligatoriu | Valoare                | Descriere                                                                                                                                                                       |
| <b>Certificate data</b>                 |             |                        |                                                                                                                                                                                 |
| Număr serial                            | Yes         | <unique_serial_number> | Număr unic al certificatului, atribuit de CA.                                                                                                                                   |
| Versiune                                | Da          | 3                      |                                                                                                                                                                                 |
| Signature Algorithm                     | Da          | SHA512                 | Algoritm de semnare conform RFC 5280.                                                                                                                                           |
| <b>Numele distinctiv al emitentului</b> |             |                        |                                                                                                                                                                                 |
| Nume Comun (CN)                         | Da          | Simplifi Root CA G1    | Numele Autorității de Certificare emitente.                                                                                                                                     |
| Organizație (O)                         | Da          | SIMPLIWORKS SRL        | Denumirea organizației emitente.                                                                                                                                                |
| Organizație Identifier (ORGID)          | Da          | VATRO-45938180         | Identificatorul organizației, diferit de denumirea acesteia. Certificatele pot include unul sau mai mulți identificatori semantici conform clauzei 5.1.4 din ETSI EN 319 412-1. |
| Țară (C)                                | Da          | RO                     | Codul de țară: RO – România (cod ISO 3166 din 2 caractere).                                                                                                                     |
| <b>Numele distinctiv al subiectului</b> |             |                        |                                                                                                                                                                                 |
| Nume Comun (CN)                         | Da          | Simplifi Root CA G1    | Numele Autorității de Certificare Rădăcină.                                                                                                                                     |
| Organizație (O)                         | Da          | SIMPLIWORKS SRL        | Denumirea organizației.                                                                                                                                                         |
| Organizație Identifier (ORGID)          | Da          | VATRO-45938180         | Identificatorul organizației, diferit de denumirea acesteia. Certificatele pot include                                                                                          |

|                                        |                                                    |                                     |                                                                          |
|----------------------------------------|----------------------------------------------------|-------------------------------------|--------------------------------------------------------------------------|
|                                        |                                                    |                                     | identificatori semantici conform ETSI EN 319 412-1.                      |
| Țară (C)                               | Da                                                 | RO                                  | Țară code: RO – Romania (2 caracter ISO 3166 Țară code)                  |
| <b>Valabilitate</b>                    |                                                    |                                     |                                                                          |
| Perioadă de valabilitate               | Da                                                 | 20 ani                              | Perioada de valabilitate a certificatului calculată de la data emiterii. |
| Nu înainte de                          | Da                                                 | <issuance_date_and_time>            | Data de început a valabilității certificatului.                          |
| Nu mai târziu de                       | Da                                                 | <issuance_date_and_time> + 20 years | Data de expirare a certificatului.                                       |
| <b>Informații despre cheia publică</b> |                                                    |                                     |                                                                          |
| Algoritm                               | Da                                                 | RSA (4096 Bits)                     | Algoritm RSA conform RFC 4055.                                           |
| Cheie publică                          | Da                                                 | <public_key>                        | Cheia publică a Autorității de Certificare Rădăcină.                     |
| <b>Extensii</b>                        |                                                    |                                     |                                                                          |
| <b>Extensii</b>                        | <b>Valori și limitări</b>                          | <b>Criticitate</b>                  | <b>Obligatoriu</b>                                                       |
| Utilizare cheie                        | keyCertSign, keyCrI Sign                           | Critic                              | Da                                                                       |
| Constrângeri de bază                   | Subject Type = CA<br>Path Length Constraint = None | Critic                              | Da                                                                       |
| Identificatorul cheii subiectului      | SHA-1 hash pe 160 biți (Key ID)                    | Non-Critic                          | Da                                                                       |

### 3.2. Profil CRL

|                      |                    |                |                                                                                    |
|----------------------|--------------------|----------------|------------------------------------------------------------------------------------|
| <b>CRL</b>           |                    |                |                                                                                    |
| <b>Câmp</b>          | <b>Obligatoriu</b> | <b>Valoare</b> | <b>Descriere</b>                                                                   |
| <b>Datele CRL</b>    |                    |                |                                                                                    |
| Versiune             | Da                 | 2              | Versiunea formatului CRL conform X.509.                                            |
| Algoritm de semnare  | Da                 | SHA512         | Algoritm de semnare conform RFC 5280.                                              |
| Perioadă de expirare | Da                 | 1 an           | Intervalul de timp în care CRL-ul este valid                                       |
| Interval de emiterie | Da                 | 1 an           | Intervalul de timp la care CRL-ul este generat și publicat.                        |
| Timp de suprapunere  | Da                 | 7 zile         | Intervalul de timp în care atât vechiul, cât și noul CRL sunt considerate valabile |

| Numele distinctiv al emitentului           |                             |                     |                                                                                                                                                               |
|--------------------------------------------|-----------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nume Comun (CN)                            | Da                          | Simplifi Root CA G1 | Numele Autorității de Certificare emitente.                                                                                                                   |
| Organizație (O)                            | Da                          | SIMPLIWORKS SRL     | Denumirea organizației emitente.                                                                                                                              |
| Organizație Identificer (ORGID)            | Da                          | VATRO-45938180      | Identificatorul organizației, diferit de denumirea acesteia. Certificatele pot include unul sau mai mulți identificatori semantici conform ETSI EN 319 412-1. |
| Țară (C)                                   | Da                          | RO                  | Codul de țară: RO – România (ISO 3166, 2 caractere).                                                                                                          |
| Extensii                                   |                             |                     |                                                                                                                                                               |
| Extensii                                   | Valori și limitări          | Criticitate         | Obligativ                                                                                                                                                     |
| Identificatorul cheii autorității emitente | 160-bit SHA-1 hash (Key ID) | Non-Critic          | Da                                                                                                                                                            |
| NumărCRL                                   | Digit starts from number 1  | Non-Critic          | Da                                                                                                                                                            |
| ExpiredCertsOnCRL                          | Da                          | Non-Critic          | Da                                                                                                                                                            |