

Profiul certificatului Autorității de Marcare Temporală

Profiluri și parametri pentru certificatul Autorității de
Marcare Temporală (TSA)

Prezentul document definește profilul
certificatului calificat utilizat de Simplifi, în
calitate de Furnizor de Servicii de Încredere
Calificat (QTSP), pentru activitățile sale de
Autoritate de Marcare Temporală (TSA). Acest

document prezintă structura și parametrii
certificatului Autorității de Marcare Temporală.

Informații despre document

Versiune	1.0
Data versiunii	1 septembrie 2025
Aprobat de	CEO
Responsabil document	Manager Servicii de Încredere
Document Name	Profilul certificatului Autorității de Marcare Temporală
Document OID	1.3.6.1.4.1.63578.1.5.4
Document Classification	Public

Istoricul documentului

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

Istoric de aprobare

Versiune	Data Aprobării	Aprobator
V 1.0	2025-09-01	CEO

Istoric de distribuire

Versiune	Data Distribuiri	Distribuit de
V 1.0	2025-09-01	Manager Servicii de Încredere

Cuprins

Informații despre document.....	2
Istoricul documentului	2
Istoric de aprobare	2
Istoric de distribuire.....	2
1. Introducere	4
2. Profil tehnic al certificatului.....	4
3. Structura certificatului	4
3.1. Profilul TSA.....	4
3.2. Profilul CRL	6

1. Introducere

Documentul descrie profilul certificatelor pentru certificatul Autorității de Marcare Temporală (TSA) și profilul CRL asociat.

2. Profil tehnic al certificatului

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

3. Structura certificatului

3.1. Profilul TSA

Certificate pentru unitatea serviciului de marcă temporală			
Câmp	Obligatoriu	Valoare	Descriere
Certificate data			
Număr serial	Da	<unique_serial_number>	Număr unic, aleatoriu, atribuit de CA
Versiune	Da	3	
Algoritm de semnare	Da	SHA512	Algoritm de semnare în conformitate cu RFC 5280
Numele distinctiv al emitentului			
Nume Comun (CN)	Da	Simplifi Qualified CA Class 3 [XX]	Numele autorității de certificare, unde [XX] este G1, G2, G3...
Organizație (O)	Da	Simplifi	Numele organizației
Identificator organizație(ORGID)	Da	VATRO-45938180	Identificarea organizației, diferită de numele organizației. 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 țării: RO – România (cod ISO 3166 din 2 caractere)
Numele distinctiv al subiectului			
Nume Comun (CN)	Da	Simplifi TSU G1	Numele unității de serviciu de marcă temporală
Țară (C)	Da	RO	Codul țării: RO – România (cod ISO 3166 din 2 caractere)
Organizație (O)	Da	SIMPLIWORKS SRL	Numele organizației

Identificator organizație(ORGID)	Da	VATRO-45938180	Identificarea organizației, diferită de numele organizației. Certificatele pot include unul sau mai mulți identificatori semantici, conform clauzei 5.1.4 din ETSI EN 319 412-1.
Valabilitate			
Perioadă de valabilitate	Da	5 years	Perioada de valabilitate a certificatului din momentul emiterii
Nu înainte de	Da	<issuance_date_and_time>	Data de început a valabilității certificatului
Nu mai târziu de	Da	<issuance_date_and_time> + 5 years	Data de expirare a valabilității certificatului
Informații despre cheia publică			
Algoritm	Da	RSA (4096 Bits)	Algoritm RSA în conformitate cu RFC 4055
Cheie publică	Da	<public_key>	Cheie publică
Extensii			
Extensii	Valori și limitări	Criticitate	Obligatoriu
Utilizare Cheie	Digital Signature	Critic	Da
Utilizare Extinsă Cheie	Time Stamping	Critic	Da
Constrângeri de bază	Subject Type= End Entity	Critic	Da
Identificatorul cheii subiectului	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Politicile certificatului	Certificate Policy [1]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/politicie	Non-Critic	Da
Identificatorul cheii autorității emitente	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Acces la informațiile autorității emitente	Method #1: CA issuer: http://simplifi.ro/pki/Simplifi_Qualified_CA_Classes_3_G1.crt Method #2: OCSP: http://simplifi.ro/ocsp	Non-Critic	Da
Puncte de distribuție CRL	http://simplifi.ro/pki/Simplifi_Qualified_CA_Classes_3_G1.crl	Non-Critic	Da

3.2. Profilul CRL

CRL			
Câmp	Obligatoriu	Valoare	Descriere
Datele CRL			
Versiune	Da	2	Versiunea formatului CRL conform X.509
Signature Algorithm	Da	SHA512	Algoritm de semnare în conformitate cu RFC 5280
Expire Period	Da	7 days	Intervalul de timp în care CRL este valabilă
Issue Interval	Da	1 day	Intervalul de timp în care CRL este generată și publicată
Overlap Time	Da	0 minutes	Intervalul de timp în care atât CRL veche, cât și cea nouă sunt valabile
Numele distinctiv al emitentului			
Nume Comun (CN)	Da	Simplifi Qualified CA Class 3 G1	Numele autorității de certificare
Organizație (O)	Da	SIMPLIWORKS SRL	Numele organizației
Identificator organizație(ORGID)	Da	VATRO-45938180	Identificarea organizației, diferită de numele organizației. 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 țării: RO – România (cod ISO 3166 din 2 caractere)
Extensii			
Extensii	Valori și limitări	Criticitate	Obligatoriu
Identificatorul cheii autorității emitente	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Număr CRL	Cifrele încep de la numărul 1	Non-Critic	Da