



Profilul certificatului calificat la Autorității de Certificare Intermediare

Profilele și parametrii Certificatelor Autorităților de
Certificare Intermediare

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

parametrii certificatului Autorității de Certificare
Intermediare.

Informații despre document

Versiune	1.0
Data Versiunii	1 septembrie 2025
Aprobat de	CEO
Responsabil de document	Manager Servicii de Încredere
Numele documentului	Profilul certificatului calificat al Autorității de Certificare Intermediare
OID Document	1.3.6.1.4.1.63578.1.5.2
Clasificare Document	Public

Istoricul documentului

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

Istoric aprobări

Versiune	Data aprobării	Aprobat de
V 1.0	2025-09-01	CEO

Istoric distribuire

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

Cuprins

Informații despre document.....	2
Istoricul documentului	2
Istoric aprobări	2
Istoric distribuire.....	2
1. Introducere	4
2. Profilul tehnic al certificatului	4
3. Structura certificatului	4
3.1. Certificat calificat al Autorității de Certificare	4
3.2. Profil CRL	6

1. Introducere

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

2. Profilul tehnic al certificatului

Certificatul este generat 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. Certificat calificat al Autorității de Certificare

Profil certificat			
Câmp	Obligatoriu	Valoare	Descriere
Certificate data			
Număr serial	Da	<unique_serial_number>	Număr unic al certificatului, atribuit de CA
Versiune	Da	3	
Algoritm de semnare	Da	SHA512	Algoritm de semnare conform RFC 5280
Numele distinctive al emitentului			
Nume comun (CN)	Da	Simplifi Root CA G1	Numele Autorității de Certificare emitente.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației emitente.
Identificator Organizație (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 (ISO 3166, 2 caractere).
Numele distinctiv al subiectului			
Nume comun (CN)	Da	Simplifi Qualified CA Class 3 {XX}	Numele Autorității de Certificare Intermediare, unde [XX] este G1, G2, G3 etc.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației.
Identificator Organizație (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 (ISO 3166, 2 caractere).
Valabilitate			
Perioadă de valabilitate	Da	10 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> + 10 years	Data de expirare a certificatului.
Informații despre cheia publică			
Algoritm	Da	RSA (4096 Bits)	Algoritm RSA conform RFC 4055.
Cheie publică	Da	<public_key>	Cheia publică a Autorității de Certificare Intermediare.
Extensii			
Extensii	Valori și limitări	Criticalitate	Obligativ
Utilizare cheie	keyCertSign, keyCrI Sign	Critic	Da
Constrângeri de bază	Subject Type = CA Path Length Constraint = 1	Critic	Da
Identificatorul cheii subiectului	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Politici de certificare	Certificate Policy [1]: 1.3.6.1.4.1.63578 . 1.1.1 CPS URI [2]: http://simplifi.ro/policies/cps	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 URI: http://Simplifi.ro/pki/Simplifi_Root_CA_G1.crt Method #2: OCSP URI:	Non-Critic	Da

	http://simplifi.ro/ocsp		
Puncte de distribuție CRL	http://simplifi.ro/pki/Simplifi_Root_CA_G1.crl	Non-Critic	Da

3.2. Profil CRL

CRL			
Câmp	Obligatoriu	Valoare	Descriere
CRL data			
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 suprapuner	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.
Identificator Organizație (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.
Country (C)	Da	RO	Codul de țară: RO – România (ISO 3166, 2 caractere).
Extensii			
Extensii	Valori și limitări	Criticalitate	Obligatoriu
Identificatorul cheii autorității emitente	SHA-1 hash pe 160 biți (Key ID)	Non-Critic	Da
Număr CRL	Numerotare secvențială începând de la 1	Non-Critic	Da
ExpiredCertsOnCRL	Da	Non-Critic	Da