

Profilul certificatelor calificate pentru utilizatorii finali

Profiluri și parametri pentru certificatele calificate
emise în conformitate cu standardele eIDAS și ETSI

Prezentul document definește profilurile certificatelor calificate utilizate de Simplifi, în calitate de Furnizor de Servicii de Încredere Calificat (QTSP). Acesta descrie structura și parametrii pentru certificatele calificate de semnătură electronică (QES) pentru persoane fizice, certificatele calificate de semnătură electronică pentru persoane fizice care acționează în numele persoanelor juridice și certificatele calificate de sigiliu electronic. De asemenea, documentul specifică profilurile de suport pentru serviciile de răspuns OCSP și emiterea CRL-urilor.

Fiecare profil este aliniat la Regulamentul eIDAS și la standarde ETSI EN 319, incluzând detalii privind convențiile de denumire a subiectului, utilizarea

cheii, perioada de valabilitate, politicile de certificare, extensiile obligatorii, precum QCStatements și referințele către PDS. Documentul include și punctele de distribuție pentru CRL, OCSP și AIA (Authority Information Access), pentru a asigura interoperabilitatea și conformitatea tehnică.

Obiectivul este furnizarea unor certificate coerente și conforme cu standardele europene, care să susțină semnătura la distanță, crearea de sigilii electronice și serviciile de revocare, garantând în același timp valabilitatea juridică pe termen lung și încrederea la nivelul Uniunii Europene.

Informații despre document

Versiune	1.0
Data versiune	1 septembrie 2025
Aprobat de	CEO
Responsabil de document	Manager Servicii de Încredere
Numele documentului	Profilul certificatelor calificate pentru utilizatorii finali
OID Document	1.3.6.1.4.1.63578.1.5.1
Clasificare Document	Public

Istoricul documentului

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

Istoricul aprobării documentului

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

Istoricul distribuirii documentului

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

Cuprins

Informații despre document.....	2
Istoricul documentului	2
Istoricul aprobării documentului.....	2
Istoricul distribuirii documentului	2
1. Introducere	4
2. Profil tehnic al certificatului.....	4
3. Corpul certificatului.....	4
3.1. Certificat calificat pentru semnătură electronică (termen lung)	4
3.2. Certificat calificat pentru semnătură electronică (persoană fizică reprezentând o persoană juridică)	6
3.3. Certificat calificat pentru sigiliu electronic.....	9
4. Profil OCSP	11
5. Profil CRL.....	12

1. Introducere

Acest document descrie profilul certificatelor pentru semnături electronice emise de Simplifi, precum și profilurile asociate listelor de revocare a certificatelor (CRL – Certificate Revocation Lists).

2. Profil tehnic al certificatului

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

3. Corpul certificatului

3.1. Certificat calificat pentru semnătură electronică (termen lung)

Următorul tabel prezintă profilul certificatului și extensiile acestuia

Semnătură electronică calificată (termen lung)			
Câmp	Obligatoriu	Valoare	Descriere
Datele certificatului			
Număr serial	Da	<unique_serial_number>	Număr unic, aleator, atribuit de către Autoritatea de Certificare (CA).
Versiune	Da	3	
Algoritm de semnare	Da	SHA512	Algoritm de semnare conform RFC 5280.
Numele Distinctiv al Emitentului (Issuer DN)			
Nume Comun(CN)	Da	Simplifi Qualified CA Class 3 [XX]	Numele Autorității de Certificare, unde [XX] reprezintă G1, G2, G3 etc.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației.
Identificator Organizație (ORGID)	Da	VATRO-45938180	Identificarea organizației distinctă de denumirea organizației. 3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.
Țară (C)	Da	RO	Codul ISO 3166 al țării: RO – România
Numele Distinctiv al Subiectului (Subject DN)			

Nume Comun(CN)	Da	<common_name>	Numele comun al subiectului, în litere latine.
Prenume (GN)	Da	<given_name>	Prenumele subiectului, în litere latine.
Nume (SN)	Da	<surname>	Numele de familie al subiectului, în litere latine.
Țară (C)	Da	RO	Codul ISO 3166 al țării: RO – România
Număr serial (SN)	Da	<serial_number>	Conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.3, Identificatorul semantic pentru persoane fizice. Un identificator pentru o persoană fizică poate fi, de exemplu: Identificatorul persoanei fizice, de exemplu: – PNORO-1234567890123 sau IDCRO-DZ123456 sau TINRO-1234567890123 (pentru identificarea bazată pe Codul Cărții de Identitate Electronice).

Valabilitate

Perioadă de Valabilitate	Da	3 years	Perioada de valabilitate a certificatului, calculată de la data emiterii.
Nu înainte de	Da	<issuance_date_and_time>	Prima zi de valabilitate a certificatului.
Nu mai târziu de	Da	<issuance_date_and_time> + 3 years	Ultima zi de valabilitate a certificatului.

Informații despre cheia publică

Algoritm	Da	RSA (2048 Bits)	Algoritm RSA conform RFC 4055.
Cheie publică	Da	<public_key>	Cheie publică a subiectului

Extensii

Extensii	Valori și limitări	Criticalitate	Obligativ
Utilizare cheie	Non-repudiation, digitalSignature	Critic	Da
Constrângeri de bază	Subject Type = End Entity	Critic	Da
Identificatorul cheii subiectului	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Politici de certificare	Certificate Policy [1]: PolicyIdentifier: 0.4.0.194112.1.2 Certificate Policy [2]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/policies	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_Class_3_G1.crt Method #2: OCSP: http://simplifi.ro/ocsp	Non-Critic	Da
Puncte de distribuție CRL	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crl	Non-Critic	Da
Nume alternativ al subiectului			
822Name	adresa de e-mail a subiectului	Non-Critic	Da
Declarații QC			
id-qcs-pkixQCSyntax-v2	0.4.0.194121.1.1 (qcSemanticsIdNatural)	Non-Critic	Da
id-etsi-qcs-QcCompliance	Da	Non-Critic	Da
id-etsi-qcs-QcSSCD	Cheia privată este stocată într-un QSCD	Non-Critic	Da
id-etsi-qcs-QcPDS	http://simplifi.ro/policies/pds language=en	Non-Critic	Da
id-etsi-qcs-QcType	id-etsi-qct-esign	Non-Critic	Da

3.2. Certificat calificat pentru semnătură electronică (persoană fizică reprezentând o persoană juridică)

Următorul tabel prezintă profilul certificatului și extensiile acestuia.

Semnătură electronică calificată (termen lung)			
Câmp	Obligatoriu	Valoare	Descriere
Datele certificatului			
Număr serial	Da	<unique_serial_number>	Număr unic, aleator, atribuit de Autoritatea de Certificare (CA).

Versiune	Da	3	
Algoritm de semnare	Da	SHA512	Algoritm de semnare conform RFC 5280.
Numele Distinctiv al Emitentului (Issuer DN)			
Nume Comun(CN)	Da	Simplifi Qualified CA Class 3 [XX]	Numele Autorității de Certificare, unde [XX] este G1, G2, G3 etc.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației emitente.
Identificator Organizație (ORGID)	Da	VATRO-45938180	Identificatorul organizației asociate persoanei fizice. Acesta reprezintă identificarea organizației distinctă de denumirea acesteia. 3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România.
Numele Distinctiv al Subiectului (Subject DN)			
Nume Comun(CN)	Da	<common_name>	Numele comun al subiectului, în litere latine.
Prenume (GN)	Da	<given_name>	Prenumele subiectului, în litere latine.
Nume (SN)	Da	<surname>	Numele de familie al subiectului, în litere latine.
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România.
Număr serial (SN)	Da	<serial_number>	Conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.3, Identificatorul semantic pentru persoane fizice. Un identificator pentru o persoană fizică poate fi, de exemplu: Identificatorul persoanei fizice, de exemplu: – PNORO-1234567890123 sau IDCRO-DZ123456 sau TINRO-1234567890123 (pentru identificarea bazată pe Codul Cărții de Identitate Electronice).
Organizație (O)	Da	<organization_name>	Denumirea organizației asociate persoanei fizice.
Identificator Organizație (ORGID)	Da	<orgid>	Identificarea organizației distinctă de denumirea organizației. 3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.

Valabilitate			
Perioadă de Valabilitate	Da	3 years	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> + 3 years	Data de expirare a certificatului.
Informații despre cheia publică			
Algoritm	Da	RSA (2048 Bits)	Algoritm RSA conform RFC 4055
Cheie publică	Da	<public_key>	Cheie publică.
Extensii			
Extensii	Valori și limitări	Criticalitate	Obligatoriu
Utilizare cheie	Non-repudiation, digitalSignature	Critic	Da
Constrângeri de bază	Subject Type = End Entity	Critic	Da
Identificatorul cheii subiectului	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Politici de certificare	Certificate Policy [1]: PolicyIdentifier: 0.4.0.194112.1.2 Certificate Policy [2]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/policies	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_Class_3_G1.crt Method #2: OCSP: http://simplifi.ro/ocsp	Non-Critic	Da
Puncte de distribuție CRL	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crl	Non-Critic	Da
Nume alternativ al subiectului			
822Name	adresa de e-mail a subiectului	Non-Critic	Da

Declarații QC			
id-qcs-pkixQCSyntax-v2	0.4.0.194121.1.1 (qcSemanticsIdNatural)	Non-Critic	Da
id-etsi-qcs-QcCompliance	Da	Non-Critic	Da
id-etsi-qcs-QcSSCD	Cheia privată este stocată într-un QSCD	Non-Critic	Da
id-etsi-qcs-QcPDS	http://simplifi.ro/policies/pds language=en	Non-Critic	Da
id-etsi-qcs-QcType	id-etsi-qct-esign	Non-Critic	Da

3.3. Certificat calificat pentru sigiliu electronic

Semnătură electronică calificată (termen lung)			
Câmp	Obligatoriu	Valoare	Descriere
Datele certificatului			
Număr serial	Da	<unique_serial_number>	Număr unic, aleator, atribuit de Autoritatea de Certificare (CA).
Versiune	Da	3	
Algoritm de semnare	Da	SHA512	Algoritm de semnare conform 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 etc.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației emitente.
Identificator Organizație (ORGID)	Da	VATRO-45938180	Identificarea organizației distinctă de denumirea organizației. 3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România.

Nume Comun(CN)	Da	<common_name>	Numele organizației (entității juridice).
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România
Organizație (O)	Da	<organization_name>	Denumirea persoanei juridice pentru care este emis certificatul calificat de sigiliu electronic.
Identificator Organizație (ORGID)	Da	<orgid>	Identificarea organizației distinctă de denumirea organizației. 3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.

Valabilitate

Perioadă de Valabilitate	Da	3 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> + 3 years	Data de expirare a certificatului.

Informații despre cheia publică

Algoritm	Da	RSA (2048 Bits)	Algoritm RSA conform RFC 4055
Cheie publică	Da	<public_key>	Cheie publică.

Extensii

Extensii	Valori și limitări	Criticalitate	Obligatoriu
Utilizare cheie	Non-repudiation, digitalSignature	Critic	Da
Constrângeri de bază	Subject Type = End Entity	Critic	Da
Identificatorul cheii subiectului	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Politici de certificare	Certificate Policy [1]: PolicyIdentifier: 0.4.0.194112.1.2 Certificate Policy [2]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/policies	Non-Critic	Da
Identificatorul cheii autorității emitente	160-bit SHA-1 hash (Key ID)	Non-Critic	Da

Acces la informațiile autorității emitente	Method #1:	Non-Critic	Da
	CA issuer:		
	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crt		
	Method #2:		
	OCSP:		
	http://simplifi.ro/ocsp		
Puncte de distribuție CRL	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crl	Non-Critic	Da
Declarații QC			
id-qcs-pkixQCSyntax-v2	0.4.0.194121.1.2 (qcSemanticsIdLegal)	Non-Critic	Da
id-etsi-qcs-QcCompliance	Da	Non-Critic	Da
id-etsi-qcs-QcSSCD	Cheia privată este stocată într-un QSCD.	Non-Critic	Da
id-etsi-qcs-QcPDS	http://simplifi.ro/policies/pds	Non-Critic	Da
	language=en		
id-etsi-qcs-QcType	id-etsi-qct-eseal	Non-Critic	Da

4. Profil OCSP

OCSP			
Câmp	Obligatoriu	Valoare	Descriere
Datele certificatului			
Număr serial	Da	<unique_serial_number>	Număr unic, aleator, atribuit de Autoritatea de Certificare (CA).
Versiune	Da	3	
Algoritm de semnare	Da	SHA512	Algoritm de semnare conform 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 etc.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației emitente.
Identificator Organizație (ORGID)	Da	VATRO-45938180	Identificarea organizației distinctă de denumirea organizației.

			3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România.
Numele distinctiv al subiectului			
Nume Comun(CN)	Da	Simplifi Qualified CA Class 3 [G1] OCSP	Numele comun al subiectului (serverul OCSP).
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației.
Valabilitate			
Perioadă de Valabilitate	Da	1 year	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> + year	Data de expirare a certificatului.
Informații despre cheia publică			
Algoritm	Da	RSA (2048 Bits)	Algoritm RSA conform RFC 4055.
Cheie publică	Da	<public_key>	Cheie publică.
Extensii			
Extensii	Valori și limitări	Criticalitate	Obligatoriu
Utilizare cheie	Digital Signature	Critic	Da
Utilizare extinsă a cheii	OCSP Signer	Non-Critic	Da
Constrângeri de bază	Subject Type = End Entity	Critic	Da
Identificatorul cheii subiectului	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Identificatorul cheii autorității emitente	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
OCSP No Check		Non-Critic	Da

5. Profil CRL

CRL			
Câmp	Obligatoriu	Valoare	Descriere
CRL data			
Versiune	Da	2	Format CRL conform X.509.

Algoritm de semnare	Da	SHA512	Algoritm de semnare conform RFC 5280.
Perioadă de expirare	Da	7 zile	Intervalul de timp în care CRL este valabil.
Interval de emiterie	Da	1 zi	Frecvența de generare și publicare a CRL.
Suprapunere	Da	0 minute	Frecvența de generare și publicare a CRL.
Numele distinctiv al emitentului			
Nume Comun(CN)	Da	Simplifi Qualified CA Class 3 {XX}	Numele Autorității de Certificare, unde [XX] este G1, G2, G3 etc.
Organizație (O)	Da	SIMPLIWORKS SRL	Denumirea organizației emitente.
Identificator Organizație (ORGID)	Da	VATRO-45938180	Identificarea organizației distinctă de denumirea organizației. 3 caractere + Codul țării + Identificatorul, conform ETSI EN 319 412-1 v1.4.4, secțiunea 5.1.4, privind identificatorul semantic pentru persoane juridice.
Țară (C)	Da	RO	Cod ISO 3166 al țării: RO – România.
Extensii			
Extensii	Valori și limitări	Criticalitate	Obligatoriu
Identificatorul cheii autorității emitente	160-bit SHA-1 hash (Key ID)	Non-Critic	Da
Număr CRL	Număr incrementeal, începând de la 1	Non-Critic	Da