Certifikačná politika Ardaco poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí

v1.0

História zmien

Verzia	Dátum vydania	Schválil	Poznámka
1.0	8.2.2022	Richard Margala	Prvá verzia dokumentu.

1 Úvod

Tento dokument definuje certifikačnú politiku (certification policy, CP) Ardaco, a.s, (ďalej aj ,,Ardaco" alebo ,,Poskytovatel"') dôveryhodných služieb definovaných v kapitole 1.1.

Základný rámec pre poskytovanie kvalifikovaných dôveryhodných služieb tvoria:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (nariadenie eIDAS)
- Zákon č. 272/2016 Z.z. z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ SR

1.1 Prehľad

Táto CP definuje pravidlá pre poskytovanie dôveryhodných služieb (alebo Signature Validation Service, ďalej len SVS)

- Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov
- Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí

1.1.1 Identifikácia TSP

Adresa sídla spoločnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovenská republika
	Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava I, v oddiely Sa, vložka číslo 2903/B.
IČO	35 829036
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com

1.1.2 Podporované politiky validačnej služby

Názov politiky (jednoznačná identifikácia)	Certifikačná politika Ardaco poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí v poslednej platnej verzii
OID	1.3.158.35829036.0.0.0.2.0 Popis použitého identifikátora objektu (OID): 1.3. – ISO Identified Organization 1.3.158. – Identifikačné číslo subjektu (IČO) 1.3.158.35829036. – Ardaco, a. s. 1.3.158.35829036.0 - Kvalifikované dôveryhodné služby

	1.3.158.35829036.0.0 – Certifikačné politiky 1.3.158.35829036.0.0.2 – CP validácie KEP a KEPe 1.3.158.35829036.0.0.2.0 – Prvá verzia

1.2 Komponenty validačnej služby

1.2.1 SVS aktéri

1.2.1.1 Poskytovateľ

Poskytovateľ je subjekt zodpovedný za poskytovanie dôveryhodných služieb podľa tejto certifikačnej politiky. V ďalšom texte je označený aj ako Signature Validation Service Provider (SVSP). SVSP má celkovú zodpovednosť za splnenie požiadaviek definovaných v danej CP ako aj v ETSI TS 119 441 V1.1. v odsekoch 5 až 8.

1.2.1.2 Odberateľ

Odberateľ je fyzická alebo právnická osoba, ktorá využíva služby podľa tejto certifikačnej politiky.

1.2.1.3 Používateľ

Používateľ je aplikácia alebo ľudská bytosť, ktorá na strane Odberateľa interagujuje s aplikáciou nad klientom na overenie podpisu (viď kapitola 1.2.2 Architektúra služby).

1.2.1.1 Iní účastníci

Iní účastníci sú:

- TSP, ktoré sú vo vzťahu podpisovateľovi/pôvodcovi pečate
  - TSP, ktorý je vydavateľom jeho certifikátu
  - akýkoľvek TSP, ktorý sa nejakým spôsobom podieľa na generovaní podpisu/pečate
  - TSP spravujúce Q(SCD) v mene podpisovateľa/pôvodcu pečate
  - TSP poskytujúce služby použitých časových pečiatok
- Poskytovatelia dôveryhodných zoznamov členských štátov EÚ
- Európska komisia poskytujúca zoznam dôveryhodných zoznamov

Participácia ďalších účastníkov je vymedzená platnými právnymi predpismi (orgán dohľadu, orgány činné v trestnom konaní, a pod).

1.2.1.2 Bezpečnostná rada

Bezpečnostná rada (ďalej len ,,Rada") prijíma dôležité opatrenia v oblasti bezpečnosti. Súčasťou Rady sú minimálne nasledovné role

- Security Officer
- Information Security Officer
- System Auditor

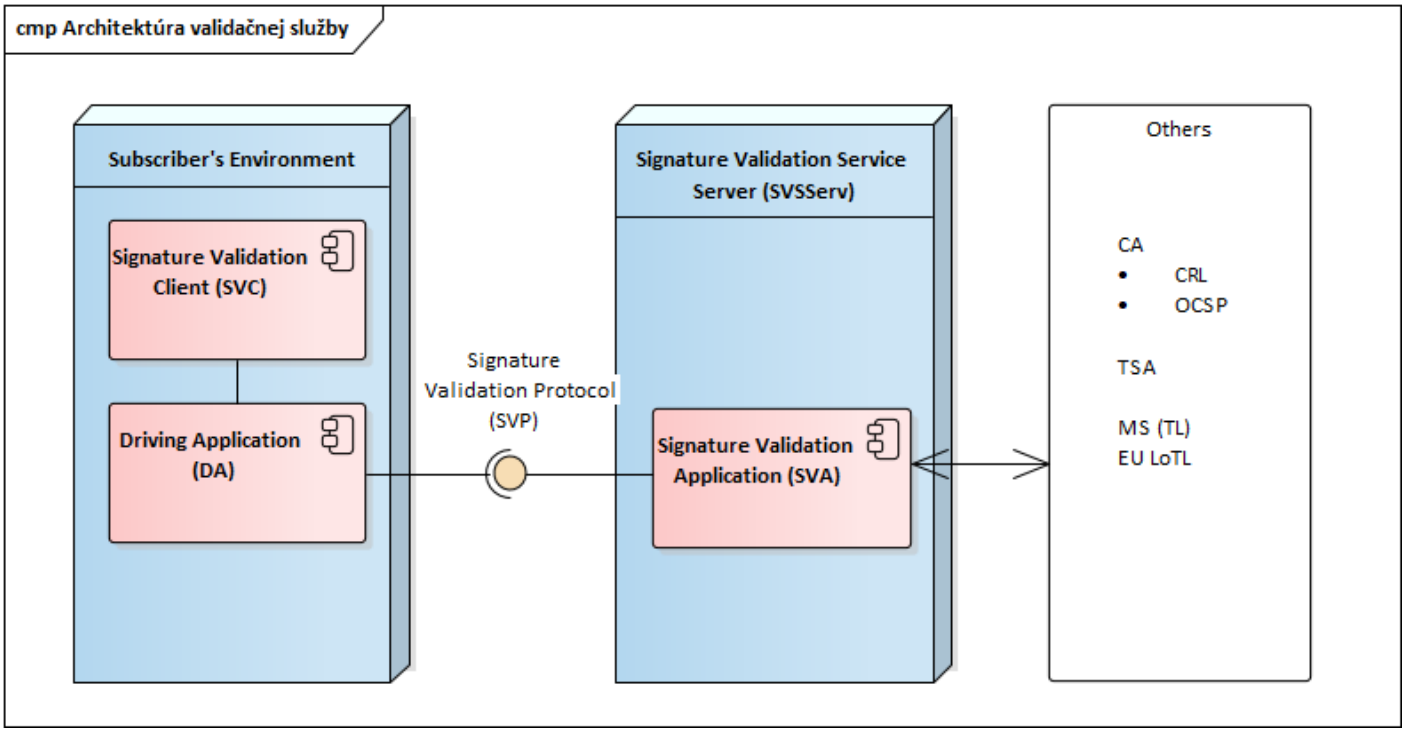
Bezpečnostná rada sa stretáva aspoň raz za 6 mesiacov aby vyhodnotila bezpečnostnú situáciu a vykonala potrebné zmeny v bezpečnostných praktikách.

Bezpečnostná rada má konečnú právomoc a zodpovednosť za špecifikáciu a schválenie certifikačných politík, pravidiel na výkon certifikačných činností (CPS) ako aj za zabezpečenie procesu preskúmania daných certifikačných politík z dôvodu ich neustálej aktuálnosti.

Členov Rady menuje a menoval prevádzkový riaditeľ.

1.2.2 Architektúra služby

Diagram nižšie zobrazuje zjednodušenú architektúru validačnej služby Ardaco:



Obrázok 1: Architektúra služby

Signature Validation Client (SVC)
Softvérový komponent, ktorý poskytuje používateľské rozhranie pre Odberateľov.

Driving Application (DA)
Aplikácia, ktorá sprostredkováva validačné funkcie pre Signature Validation Client.

Signature Validation Service Protocol (SVP)
Protokol na výmenu informácií s Signature Validation Service Server (SVSServ) cez bezpečný komunikačný kanál.

Signature Validation Service Server (SVSServ)
Komponent, ktorý implementuje SVP na strane SVSP.

Signature Validation Application (SVA)
Softvérový komponent, ktorý je zodpovedný za validáciu podpisu/pečate a ktorý implementuje overovací algoritmus a vytvára správu s overenia.

1.3 Definície a skratky

1.3.1 Definície

Na účely tohto dokumentu sú termíny a definície uvedené v norme ETSI EN 319 401 [2], v ETSI TR 119 001 [i.2] ako aj nižšie v slovenskom ako aj anglickom jazyku pre lepšiu interpretáciu:

kontrola použiteľnosti: určenie, či podpis vyhovuje pravidlám použiteľnosti podpisu

POZNÁMKA 1. – Kontrola použiteľnosti je širší pojem ako validácia, ako sa uvádza v tomto dokumente: je mimo rozsahu tohto dokumentu.

POZNÁMKA 2. – Kontrola použiteľnosti môže byť poskytnutá ako doplnok k službe overovania podpisu definovanej v tomto dokumente.

applicability checking: determination whether a signature conform to signature applicability rules

NOTE 1: The applicability checking is a broader concept than validation as covered by the present document: it is out of scope of the present document.

NOTE 2: The applicability checking can be provided as an adjunct to the signature validation service defined in the present document.

(podpis) typ záväzku: podpisom akceptovaný údaj o presnej implikácii digitálneho podpisu
(signature) commitment type: signer-accepted indication of the exact implication of a digital signature

(podpis) obmedzenia tvorby: kritériá používané pri vytváraní digitálneho podpisu
(signature) creation constraint: criteria used when creating a digital signature

aplikácia: aplikácia, ktorá používa systém na vytváranie podpisov na vytvorenie podpisu alebo aplikáciu na overenie podpisov na overenie digitálnych podpisov alebo aplikácia na rozšírenie podpisov na rozšírenie digitálnych podpisov

POZNÁMKA: V procese overovania podpisu poskytuje vodičská aplikácia (DA) digitálny podpis AdES a ďalší vstup do aplikácie na overovanie podpisu (SVA).

driving application: application that uses a signature creation system to create a signature or a signature validation application in order to validate digital signatures or a signature augmentation application to augment digital signatures

NOTE: In a signature validation process, the driving application (DA) provides AdES digital signature and other input to a signature validation application (SVA).

kvalifikovaná validačná služba pre kvalifikované elektronické pečate: Ako sa uvádza v článku 40 nariadenia (EÚ) č. 910/2014 [i.1].
qualified validation service for qualified electronic seals: As specified in Regulation (EU) No 910/2014 [i.1], Article 40.

kvalifikovaná služba overovania pre kvalifikované elektronické podpisy: Ako sa uvádza v článku 33 nariadenia (EÚ) č. 910/2014 [i.1].
qualified validation service for qualified electronic signatures: As specified in Regulation (EU) No 910/2014 [i.1], Article 33.

kvalifikovaný poskytovateľ validačných služieb: SVSP, ktorý poskytuje kvalifikovanú validačnú službu pre kvalifikované elektronické pečate alebo kvalifikovanú validačnú službu pre kvalifikované elektronické podpisy
qualified validation service provider: SVSP that provides qualified validation service for qualified electronic seals or qualified validation service for qualified electronic signatures

akceptovanie podpisu: technické overenie, ktoré sa má vykonať na vlastnom podpise alebo na atribútoch podpisu (t. j. „obmedzenia prvkov podpisu“)

POZNÁMKA: Akceptácia podpisu je technický proces definovaný a špecifikovaný v ETSI TS 119 102-1 [3] a vykonávaný aplikáciou na overenie podpisu (je teda jednou súčasťou procesu overenia podpisu). Túto aplikáciu na overenie podpisu možno spravovať SVSP alebo môže ísť o samostatnú aplikáciu v prostredí spoliehajúcej sa strany.

signature acceptance: technical verification to be performed on the signature itself or on the attributes of the signature (i.e. the „signature elements constraints“)

NOTE: The signature acceptance is a technical process defined and specified in ETSI TS 119 102-1 [3] and performed by a signature validation application (it is thus one part of the signature validation process).This signature validation application can be managed by a SVSP or can be a stand-alone application on the relying party environment..

pravidlá použiteľnosti podpisu: súbor pravidiel použiteľných pre jeden alebo viacero digitálnych podpisov, ktoré definujú požiadavky na určenie, či je podpis vhodný na konkrétny obchodný alebo právny účel

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose

trieda podpisov: množina podpisov dosahujúcich danú funkčnosť

PRÍKLAD: Podpis s časom, podpis s dlhodobým overovacím materiálom, Podpis poskytujúci dlhodobú dostupnosť a integritu overovacieho materiálu sú možné triedy podpisu.

signature class: set of signatures achieving a given functionality

EXAMPLE: Signature with time, signature with long term validation material, Signature providing Long Term Availability and Integrity of Validation Material are possible signature classes.

zariadenie na vytváranie podpisov: nakonfigurovaný softvér alebo hardvér používaný na implementáciu údajov na vytvorenie podpisu a na vytvorenie aplikácie na overenie podpisu hodnoty digitálneho podpisu: aplikácia, ktorá overí podpis podľa politiky overovania podpisu a ktorá vydáva indikáciu stavu (tj stav overenia podpisu) a správu o overení podpisu

POZNÁMKA. – Aplikácia overovania podpisu (SVA) je špecifikovaná v ETSI TS 119 102-1 [3].

signature creation device: configured software or hardware used to implement the signature creation data and to create a digital signature value signature validation application: application that validates a signature against a signature validation policy, and that outputs a status indication (i.e. the signature validation status) and a signature validation report

NOTE: The signature validation application (SVA) is specified in ETSI TS 119 102-1 [3].

klient na overenie podpisu: komponent alebo softvér, ktorý implementuje protokol overovania podpisov na užívateľskej strane

signature validation client: component or piece of software that implements the signature validation protocol on the user‘s side

politika overovania podpisov: súbor obmedzení overovania podpisov, ktoré spracováva alebo má spracovať SVA

signature validation policy: set of signature validation constraints processed or to be processed by the SVA

zobrazenie overovania podpisu: voliteľný prvok v procese overovania podpisu, ktorý môže overovateľ použiť na kontrolu výsledkov procesu overovania

signature validation presentation: optional element in the signature validation process that can be used by a verifier to check the results of a validation process

správa o overení podpisu: komplexná správa o overení, ktorú poskytuje aplikácia na overenie podpisu pre DA a ktorá umožňuje aplikácii a ktorejkoľvek inej strane kontrolovať podrobnosti o rozhodnutiach prijatých počas overovania a skúmať podrobné príčiny poskytnutej indikácie stavu pomocou aplikácie na overenie podpisu

PRÍKLAD: Článok 5.1.3 ETSI TS 119 102-1 [3] špecifikuje minimálne požiadavky na obsah takejto správy a ETSI TS 119 102-2 [i.3] špecifikuje takúto správu.

signature validation report: comprehensive report of the validation provided by the signature validation application to the DA and allowing the driving application and any party beyond the driving application, to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the signature validation application

EXAMPLE: Clause 5.1.3 of ETSI TS 119 102-1 [3] specifies minimum requirements for the content of such a report and ETSI TS 119 102-2 [i.3] specifies such a report.

Politika služby overovania podpisov (SVS): súbor pravidiel, ktoré označujú použiteľnosť služby overovania podpisov pre konkrétnu komunitu a/alebo triedu aplikácií so spoločnými bezpečnostnými požiadavkami

POZNÁMKA: Politika SVS sa vzťahuje na službu; je to špecifická podtrieda politiky dôveryhodných služieb, ako je definovaná v ETSI EN 319 401 [2]. Týka sa to kvality a použiteľnosti služby

Signature Validation Service (SVS) policy: set of rules that indicates the applicability of a signature validation service to a particular community and/or class of application with common security requirements

NOTE: A SVS policy is applicable to a service; it is a specific sub-class of trust service policy as defined in ETSI EN 319 401 [2]. It relates to the quality and applicability of the service

vyhlásenie o praxi služby overovania podpisov (SVS): vyhlásenie o postupoch a procedúrach používaných na riešenie všetkých požiadaviek identifikovaných na poskytovanie služby overovania podpisov

POZNÁMKA: Vyhlásenie o postupe overovania podpisov je vyhlásenie o postupe dôveryhodných služieb, ktoré je súčasťou dokumentácie SVSP (pozri ETSI EN 319 401 [2])

signature validation service (SVS) practice statement: statement of the practices and procedures used to address all the requirements identified for the provision of the signature validation service

NOTE: A signature validation service practice statement is a trust service practice statement that is part of the SVSP's documentation (see ETSI EN 319 401 [2])

server služby overovania podpisov: komponent, ktorý implementuje protokol overovania podpisov a spracováva overovanie podpisov na strane SVSP

signature validation service server: component that implements the signature validation protocol and processes the signature validation on the SVSP‘s side

stav overenia podpisu: jeden z nasledujúcich indikátorov: CELKOM PREJDENÉ, CELKOVÉ ZLYHANIE alebo NEURČITÉ

signature validation status: one of the following indications: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE

validácia podpisu: proces overovania a potvrdenia, že digitálny podpis je technicky platný

signature validation: process of verifying and confirming that a digital signature is technically valid

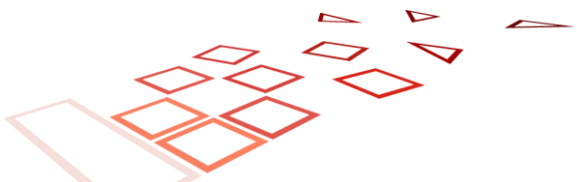
overenie podpisu: proces kontroly kryptografickej hodnoty podpisu pomocou overenia podpisu

signature verification: process of checking the cryptographic value of a signature using signature verification data

podpisovateľ: subjekt, ktorý je tvorcom digitálneho podpisu

signer: entity being the creator of a digital signature

obmedzenie overovania podpisu: technické kritériá, podľa ktorých môže byť digitálny podpis overený, napr. ako je špecifikované v ETSI TS 119 102-1 [3]



signature validation constraint: technical criteria against which a digital signature can be validated, e.g. as specified in ETSI TS 119 102-1 [3]

užívateľ: aplikácia alebo človek interagujúci s aplikáciou nad overením podpisu validácia klienta: proces overovania a potvrdenia platnosti certifikátu alebo digitálneho podpisu
user: application or human being interacting with an application on top of a signature validation client validation: process of verifying and confirming that a certificate or a digital signature is valid

validačné dáta: dáta, ktoré sa používajú na validáciu digitálneho podpisu
validation data: data that is used to validate a digital signature

validácia kvalifikovaného elektronického podpisu: Ako sa uvádza v článku 32 nariadenia (EÚ) č. 910/2014 [i.1].
validation of qualified electronic signature: As specified in Regulation (EU) No 910/2014 [i.1], Article 32.

validácia kvalifikovaných elektronických pečatí: Ako sa uvádza v článku 40 nariadenia (EÚ) č. 910/2014 [i.1].
validation of qualified electronic seals: As specified in Regulation (EU) No 910/2014 [i.1], Article 40.

overovacia služba: systém prístupný cez komunikačnú sieť, ktorý overuje digitálny podpis: subjekt, ktorý chce overiť alebo overiť digitálny podpis
validation service: system accessible via a communication network, which validates a digital signature verifier: entity that wants to validate or verify a digital signature

1.3.2 Skratky

CA	Certifikačná autorita
CP	Certifikačná politika
CPS	Pravidlá pre výkon certifikačných činností
CRL	Zoznam znevládnených certifikátov (Certification Revocation List)
ČP	Časová pečiatka
KC	Kvalifikovaný certifikát
KEP	Kvalifikovaný elektronický podpis
KEPe	Kvalifikovaná elektronická pečať
PKI	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
RA	Registračná autorita
QSCD	Zariadenia na vyhotovenie kvalifikovaného elektronického podpisu (Qualified Signature Creation Device)
SVSP	Poskytovateľ služieb validácie kval. Podpisov a pečatí

1.4 Politiky a postupy

1.4.1 Organizácia spravujúca TSP dokumentáciu

Tabuľka obsahuje údaje Poskytovateľa, ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

Adresa sídla spoločnosti	Ardaco, a.s.

	Polianky 5 841 01 Bratislava Slovenská republika
	Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava I, v oddiely Sa, vložka číslo 2903/B.
IČO	35 829036
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com

1.4.2 Kontaktná osoba

Na účel tvorby politík má Poskytovateľ vytvorenú samostatnú autoritu pre správu politík (Bezpečnostná rada viď CPS), ktorá plne zodpovedá za jej obsah, a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík Poskytovateľa.

Tabuľka obsahuje kontaktné údaje na zložku zodpovednú za prevádzku certifikačných autorít Poskytovateľa.

Adresa sídla spoločnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovenská republika
	Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava I, v oddiely Sa, vložka číslo 2903/B.
IČO	35 829036
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com
E-mail pre nahlasovanie incidentov:	incidents@ardaco.com
Tel. číslo:	+421 2 3221 2311

1.4.3 Uplatniteľnosť (verejnej) dokumentácie Poskytovateľa

Poskytovateľ ako aj organizácia spravujúca TSP dokumentáciu má definované nasledovné dokumenty súvisiacich s SVS, ktoré publikuje na webovom sídle spoločnosti https://tsp.ardaco.com:

1. Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

Názov dokument a jednoznačná identifikácia	Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok v poslednej platnej verzii
OID	1.3.158.35829036.0.0.0.1.0 Popis použitého identifikátora objektu (OID): 1. – ISO assigned OIDs 1.3. – ISO Identified Organization 1.3.158. – Identifikačné číslo subjektu (IČO)

	1.3.158. 35829036. – Ardaco, a.s. 1.3.158. 35829036.0.0.0.1. - CA Ardaco,a.s – vyhotovovanie kvalifikovaných certifikátov 1.3.158. 35829036.0.0.0.1.0 – CP TSA Ardaco, a.s.
Link:	https://www.qsign.sk/download/tsp/ardaco_tsa_cp.pdf

2. Certifikačná politika Ardaco pre služby vyhotovovania a overovania kvalifikovaných certifikátov

Názov dokumentu (jednoznačná identifikácia)	Certifikačná politika pre vydávania a overovania kvalifikovaných certifikátov v poslednej platnej verzii
OID	1.3.158.35975946.0.0.0.0.0 Popis použitého identifikátora objektu (OID): 1.3. – ISO Identified Organization 1.3.158. – Identifikačné číslo subjektu (IČO) 1.3.158. 35829036. – Ardaco, a. s. 1.3.158. 35829036.0.0.0.0.– CA Ardaco, a.s. 1.3.158.35975946.0.0.0.0.0 – CP CA Ardaco, a.s
Link:	https://www.qsign.sk/download/tsp/ardaco_cp_qtsp_qc.pdf

3. Politika Ardaco pre služby vyhotovovania a overovania kvalifikovaných certifikátov

Názov dokumentu (jednoznačná identifikácia)	Politika Ardaco pre KC pre vyhotovovania a overovania kvalifikovaných certifikátov v poslednej platnej verzii
OID	Neudeľuje sa
Link:	https://www.qsign.sk/download/tsp/ardaco_tsp_politika_pre_kc.pdf

4. Pravidlá na výkon certifikačných činností (CPS) Ardaco

Názov dokumentu (jednoznačná identifikácia)	Pravidlá na výkon certifikačných činností (CPS) Ardaco v posledne platnej verzii
OID	Neudeľuje sa
Link:	https://www.qsign.sk/download/tsp/ardaco_tsp_cps.pdf

5. Všeobecné podmienky používania

Názov dokumentu (jednoznačná identifikácia)	Všeobecné podmienky používania v posledne platnej verzii
OID	Neudeľuje sa
Link:	https://www.qsign.sk/doc/vseobecne_podmienky_pouzivania.pdf

6. Zásady ochrany osobných údajov Ardaco

Názov dokumentu (jednoznačná identifikácia)	Zásady ochrany osobných údajov Ardaco v posledne platnej verzii
OID	Neudeľuje sa
Link:	https://www.qsign.sk/doc/zasady_ochrany_osobnych_udajov.pdf

1.4.3.1 Bezpečnostná politika

Organizácia má definovanú politiku bezpečnosti informácií ako samostatný dokument, ktorá je schválená vedením organizácie, ktorá stanovuje prístup organizácie k riadeniu jej informačnej bezpečnosti.

Zmeny v politike bezpečnosti informácií sa v prípade potreby oznamuje tretím stranám (predplatiteľom, spoliehajúcim sa stranám, hodnotiacim orgánom, dozorným alebo iným regulačným orgánom).

Politika bezpečnosti informácií je teda zdokumentovaná, implementovaná a udržiavaná vrátane bezpečnosti kontroly a prevádzkové postupy pre zariadenia, systémy a informačné aktíva organizácie poskytujúce dôveryhodné služby. Taktiež je zverejnená a oznámená všetkým zamestnancom, ktorých sa to týka.

Politika bezpečnosti informácií a súpis aktív pre informačnú bezpečnosť je pravidelne preskúmavaná v plánovaných intervaloch alebo ak dôjde k významným zmenám s cieľom zabezpečiť ich nepretržitú vhodnosť a primeranosť a efektívnosť. Všetky zmeny, ktoré majú vplyv na úroveň poskytovanej bezpečnosti, sú schválené.

Konfigurácia systémov je taktiež pravidelne kontrolovaná na zmeny, ktoré porušujú bezpečnostné politiky.

1.4.3.2 Risk Assesment

Poskytovateľ vykoná posúdenie rizika s cieľom identifikovať, analyzovať a vyhodnotiť riziká dôveryhodných služieb s prihliadnutím na obchodné a technické problémy. Následne identifikuje a vyberie vhodné opatrenia na ošetrenie rizika s prihliadnutím na výsledky posúdenia rizika. Opatrenia na ošetrenie rizika zabezpečia, aby úroveň bezpečnosti bola primeraná stupňu rizika.

Rizikový manažment je plne integrovaný v rámci existujúcich procesov riadených podľa normy ISO9001 s integrovanými vybranými a platnými postupmi definovanými normou ISO27005.

1.4.3.2.1 Posúdenie rizík

Poskytovateľ minimálne počas preskúmania manažmentom posudzuje organizačné riziká pričom uchováva aj zdokumentované informácie. Ďalšia možnosť posudzovania rizika je pravidelne počas projektovej porady ako aj počas porád jednotlivých oddelení organizácie. Následne riziká sú ošetrované priebežne podľa výskytu a vlastníka .

Projektové riziká sú zaznamenávané v rámci dokumentu „Risk assessment“. IT riziká (do danej skupiny patria aj bezpečnostné riziká) sú evidované na procesnom portály , aby bolo zabezpečené riešenie na úrovni manažmentu. Takto odsúhlasené kroky sú následne evidované v internom systéme alebo vytvorením samostatného interného projektu.

Kompletný proces postup je definovaný v samostatnom dokumente s názvom „Risk Manažment“.

1.4.3.3 Referencie

[1] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".
[2] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[3] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
[4] ISO/IEC 15408 part 1 to 3: "Information technology -- Security techniques -- Evaluation criteria for IT security".
[5] ISO/IEC 19790: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[6] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules".
[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".
[i.3] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report"

1.4.4 Vyhlásenie o postupe služby overovania podpisov (Signature Validation Service practice statement)

Uplatňujú sa požiadavky špecifikované v dokumente 3. Politika Ardaco pre služby vyhotovovania a overovania kvalifikovaných certifikátov (viď kapitola 1.4.3) kap. 6.1.

Okrem toho platia aj tieto osobitné požiadavky:

- Vyhlásenie o postupe SVS je štruktúrované podľa normy ETSI TS 119 441 V1.1.1 prílohy A .
- Vyhlásenie o postupe SVS uvádza, sa odkazuje a stručne opisuje podporované zásady SVS.
- SVSP v danom vyhlásení okrem dodávateľa cloud služieb, ktorý je zmluvne zabezpečený dodržiavať príslušné zásad a postupy SVSP pre ňu relevantné , neeviduje iné externé organizácií, ktoré podporujú jej služby.

1.4.5 Zmluvné podmienky (Terms and Condition)

Uplatňujú sa požiadavky špecifikované v dokumente 3. Politika Ardaco pre služby vyhotovovania a overovania kvalifikovaných certifikátov (viď kapitola 1.4.3) kap. 6.2. Taktiež sú definované licenčné podmienky ako aj iné zmluvné podmienky, ktoré sú prístupné a dodávané s SVS.

2 Riadenie a prevádzka dôveryhodnej služby

2.1 Interná organizácia

2.1.1 Spoľahlivosť organizácie

Uplatňujú sa ustanovenia CPS, kap. 9.2 až 9-9 a 9.16.

2.1.2 Oddelenie rolí

Uplatňujú sa ustanovenia CPS, kap. 5.5.

2.2 Ľudské zdroje

Uplatňujú sa ustanovenia CPS, kap. 5.6.

2.3 Správa aktív

2.3.1 Všeobecné požiadavky

Uplatňujú sa ustanovenia CPS, kap. 5.3.1.

2.3.2 Nakladanie s médiami

Uplatňujú sa ustanovenia CPS, kap. 5.3.2.

2.4 Riadenie prístupu

Uplatňujú sa ustanovenia CPS, kap. 5.4.2 a 5.5.3

2.5 Kryptografické opatrenia

Uplatňujú sa ustanovenia CPS, kap. 6.2 až 6.4.

Pre účely pečatenia správ z validácie používa súkromný kľúč patriaci v verejnému certifikátu Poskytovateľa, ktorý je vyhradený pre tento účel. Životný cyklus tohto súkromného kľúča a certifikátu sa riadi uvedenými ustanoveniami. Kľúč je uložený v kryptografickom module, ktorý je posúdený na úroveň EAL 4+ a spĺňa požiadavky FIPS PUB 140-2, level 3.

2.6 Fyzická a priestorová bezpečnosť

Uplatňujú sa ustanovenia CPS, kap. 5.4.

2.7 Prevádzková bezpečnosť

Uplatňujú sa ustanovenia CPS, kap. 5.5.

2.8 Sieťová bezpečnosť

Uplatňujú sa ustanovenia CPS, kap. 6.7.

2.9 Riadenie incidentov

Uplatňujú sa ustanovenia CPS, kap. 5.10.1.

2.10 Zber dôkazov

Uplatňujú sa ustanovenia CPS. kap. 5.7.

Okrem dôkazov uvedených v danej kapitole sa zaznamenáva každá validácia podpisu/pečate. Zaznamenáva sa presný čas, typ udalosti, identifikácia Odberateľa a správa z validácie (ak ju systém úspešne vygeneroval).

2.11 Riadenie biznis kontinuity

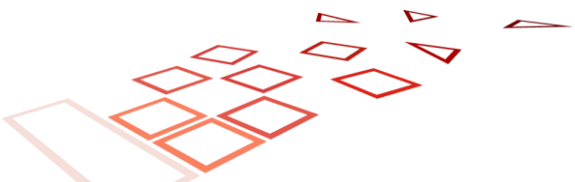
Uplatňujú sa ustanovenia CPS, kap. 5.10.4.

2.12 Ukončenie činnosti TSP a plán ukončenia

Uplatňujú sa ustanovenia CPS, kap. 5.11. Poskytovateľ má spracovaný Plán ukončenia činnosti v internom dokumente.

2.13 Súlad

Uplatňujú sa ustanovenia CPS, kap. 8.



3 Dizajn validačnej služby

3.1 Požiadavky na validačný proces

Validačná služba pri vyhodnocovaní platnosti elektronického podpisu/pečate postupuje podľa pravidiel popísaných v [ETSI TS 119 102].

Komunikácia pri využití validačnej služby prebieha v nasledovných krokoch:

1. Na strane Odberateľa sa vygeneruje a odošle požiadavka na validáciu
2. SVSServ vykoná validačný proces.
3. SVSServ pripraví a odošle validačnú správu.
4. Prezentácia validačnej správy na strane Odberateľa.

Pri využívaní validačnej služby je potrebné dodržať podmienky použitia a obmedzenia uvedené v ďalších sekciách.

3.1.1 Obmedzenia pre validáciu

3.1.1.1 Všeobecné obmedzenia

Obmedzenie	Hodnota
Veľkosť súboru	Definované aktuálnou verziou integračnej príručky.

3.1.1.2 Podporované typy formátov elektronických podpisov a pečatí

Podporované sú nasledovné typy formátov podpisov a podpisových kontajnerov

- ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
- ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
- ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
- ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

3.1.1.3 Obmezenia na podporované elektronické podpisy a pečate

Obmedzenie	Hodnota
Overovanie vnorených podpisových kontajnerov	Nie

3.1.1.4 Obmedzenia na podpísané údaje

Constraint(s)	Constraint value at signature validation

(b)1. ConstraintOnDTBS: This constraint indicates requirements on the type of the data to be signed.	Nie
(b)2.ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicate the required content related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This includes:	
(b)2.1 MandatedSignedQProperties-DataObjetFormat to require a specific format for the content being signed by the signer.	Nie
(b)2.2 MandatedSignedQProperties-content-hints to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer.	Nie
(b)2.3 MandatedSignedQProperties-content-reference to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc.	Nie
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • whole: the whole data has to be signed; • parts: only certain part(s) of the data have to be signed. In this case additional information should be used to express which parts have to be signed.	Nie

3.1.1.5 Obmedzenia pre X.509 validáciu

Constraint(s)	Constraint value at signature validation
(m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process. Such TAs should be provided in the form of (self-signed) certificates (see clause 6.1.1 of IETF RFC 5280 [i.13] on how to treat such certificates as conveyor of TA information) and a time until when these trust anchors were considered reliable.	EU TSL
(m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any.	None
(m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) [i.13].	None

(m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) [i.13].	None
(m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) [i.13].	None
(m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) [i.13].	None
(m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) [i.13].	None
(m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) [i.13]	None
(m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path [i.13]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it).	None
(m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates [i.13]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values appearing in certificate of authorities in the certification path).	None
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process [i.13]. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows:	
(m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used	eitherCheck (Either OCSP or CRL checks shall be carried out)
(m)2.2 RevocationFreshnessConstraints: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation (see [i.4]) or require the SVA to only accept revocation information issued a certain time after the signature has been created	None
(m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification	None

authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.	

3.1.1.6 Kryptografické obmedzenia

Constraint(s)	Constraint value at signature validation
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps).	Podľa [ETSI TS 119 312].

3.2 Požiadavky na validačný protokol

Validačný protokol je definovaný v samostatnej príručke.[1]

3.3 Rozhrania

3.3.1 Komunikačný kanál

Komunikácia medzi validačným serverom (SVSP) a klientom musí prebiehať prostredníctvom zabezpečeného kanála (šifrovanie).

SVSP môže vyžadovať autentifikáciu klienta.

3.3.2 SVSP – iní TSP

Pri prípadnej komunikácii medzi SVSP a inými TSP (napr. využitie externej TSA) sa uplatňujú opatrenia podľa 3.3.1.

3.4 Požiadavky na validačnú správu

Výsledkom kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí je správa z validácie, ktorá môže byť vytvorená v nasledovných formátoch:

- TXT súbor v UTF-8 kódovaní vo formáte podľa SD 5.3 umiestnený v ASiC kontajneri
- XML súbor vo formáte podľa ETSI TS 119 102-2

[1] QSign 6.0 AS – Programátorská príručka.

V oboch prípadoch je validačná správa autorizovaná Poskytovateľom kľúčom patriacim k certifikátu, ktorý je vyhradený na tento účel (min. na úrovni podpisu/pečate,,zdokonalená") a opatrená časovou pečiatkou.

Ak služba nie je schopná validačnú správu vygenerovať (napr. nedodržanie podmienok služby alebo výpadok interných služieb), vráti chybový kód z popisom dôvodu.