Disig, a.s.

SWACA 3.0

Softvér pre certifikačnú autoritu

SWACA 3.0 je robustný, škálovateľný, komplexný a modulárny informačný softvérový systém pre prevádzku certifikačných autorít (CA) umožňujúci poskytovanie dôveryhodných služieb a kvalifikovaných dôveryhodných služieb v zmysle nariadenia eIDAS a podporných služieb spojených s elektronickým podpisom a elektronickým obehom dokumentov, vrátane zabezpečenia správy celého životného cyklu certifikátov (vydanie, zrušenie, exspirácia, uchovávanie záznamov), integráciu s bezpečnostným hardvérom a zaznamenávanie auditných záznamov pre všetky významné činnosti systému.

Vlastnosti a výhody

Súlad s nariadením 910/2014 (eIDAS) – umožňuje poskytovať kvalifikované dôveryhodné služby.

Bezpečnosť – integrácia s certifikovanými HSM zariadeniami, prísna autentifikácia operátorov.

Modulárnosť – nasadenie len potrebných komponentov podľa scenára.

Škálovateľnosť – vhodné od menších CA až po národné projekty.

Auditovateľnosť – spĺňa legislatívne a regulačné požiadavky na prevádzku CA.

Profil spoločnosti

Disig, a.s. je slovenský líder v oblasti poskytovania dôveryhodných služieb, elektronického podpisu a infraštruktúry verejných kľúčov (PKI). Jeho dlhoročná expertíza je potvrdená medzinárodne uznávanými certifikáciami, ktoré priamo súvisia s vývojom, prevádzkou a podporou riešenia SWACA 3.0.

Disig, a.s. je držiteľom ISO certifikátov pre viaceré manažerské systémy, ktoré v praxi dokazujú, že spoločnosť je schopná zabezpečiť bezpečný vývoj, spoľahlivú prevádzku a dlhodobú podporu SWACA 3.0 v súlade s najvyššími požiadavkami na dôvernosť, integritu, dostupnosť a bezpečnosť.

ISO 9001

ISO/IEC 27001

ISO/IEC 20000-1

ISO 14001

ISO 22301

ISO/IEC 27701

Architektúra a komponenty SWACA 3.0

Modulárny návrh systému SWACA umožňuje nasadenie nasledovných častí:

1. SWACA Core - CA modul (Certification Authority) – základný modul na vyhotovovanie certifikátov a vyhotovovanie CRL
2. RA modul (Registration Authority) – Registrácia žiadostí o certifikát a osobných údajov žiadateľa o certifikát
3. OCSP Responder – online overovanie platnosti certifikátov
4. TSA modul – poskytovanie časových pečiatok
5. Audit & Compliance – kompletná evidencia všetkých činností v systéme
6. Používateľské portály – portál pre používateľov na rôzne činnosti vykonávané počas životného cyklu certifikátu
7. RA Client– softvérová aplikácia pre pracovníkov registračnej autority
8. PKI klient – softvérová aplikácia pre koncové pracovné stanice
9. PKI Server – serverový komponent v rámci SWACA, ktorá sprostredkúva komunikáciu medzi PKI klientom a systémom SWACA
10. CKAS Server – vykonáva bezpečné zálohovanie a obnovu šifrovacích kľúčov používateľov

Ďalšie moduly

11. Disig Charon – jednosmerný prenos dát medzi galvanicky oddelenými sieťami.
12. Disig Web Signer – webové riešenie pre kvalifikovaný elektronický podpis/pečať
13. Disig QES Signer – serverové riešenie pre kvalifikovaný elektronický podpis/pečať
14. Disig QES Portal – portálové riešenie pre kvalifikovaný elektronický podpis/pečať
15. Disig Enterprise Signer – portálové riešenie pre elektronické podpisovanie dokumentov medzi partnermi
16. Disig eArchive – zabezpečuje dlhodobú overiteľnosť archivovaných dokumentov podpísaných QES
17. Disig Remote Signing – vyhotovovanie kvalifikovaného elektronického podpisu na diaľku
18. Disig Validation Service - overovanie platnosti elektronických podpisov a pečatí v súlade s nariadením eIDAS

Detailný popis modulov SWACA 3.0

1. SWACA Core - CA modul (Certification Authority)

Technická špecifikácia

Základný modul na vyhotovovanie certifikátov a vyhotovovanie CRL prostredníctvom kryptografických kľúčov uložených v HSM v súlade s požiadavkami nariadenia eIDAS a ETSI štandardov.

Hlavné funkcie:

Vyhotovovanie certifikátov a vyhotovovanie CRL
Správa politiky CA
Administrátorské rozhranie pre správu politík CA
Podpora rôznych typov CA a rôznych typov certifikátov
Publikovanie CRL cez SFTP alebo LDAP/HTTP
Auditné záznamy

Použitie:

Vyhotovovanie certifikátov a kvalifikovaných certifikátov a CRL
Centrálna riadiaca vrstva
Nastavenie politík a procesov
Rozhranie pre administrátorov pre správu politík

Funkčný opis

Základná časť systému na vyhotovovanie a rušenie certifikátov.

Hlavné prínosy:

Jednotná správa viacerých CA
Jednoduchý dohľad nad systémom vyhotovovania certifikátov
Súlad s eIDAS
Auditovateľnosť
Dôveryhodnosť

Oblasti využitia:

Prevádzka CA pre kvalifikované dôveryhodné služby a dôveryhodné služby
Národné CA projekty
Podnikové CA

2. RA modul (Registration Authority)

Technická špecifikácia

Registrácia žiadostí o certifikát a osobných údajov žiadateľa o certifikát.

Hlavné funkcie:

Prijímanie žiadostí
Registrácia osobných údajov
Príprava podkladov pre vyhotovenie certifikátu v CA
Auditovanie

Použitie:

Funkčný opis

Registrácia žiadostí a údajov potrebných k overeniu žiadateľa certifikátu.

Hlavné prínosy:

Uchovávanie údajov z overenia identity
Oddelenie procesov spracovávania osobných údajov
Jednoduchšie služby

Oblasti využitia:

Oddelenie registračných procesov pre interné potreby klientov
Bezpečnostná separácia osobných údajov
Integrácia s klientskymi systémami

Front-office banky/poisťovne
eGovernment
Podniky s veľkým množstvom používateľov

3. OCSP Responder

Technická špecifikácia

OCSP Responder zabezpečuje online overovanie platnosti certifikátov podľa štandardu RFC 6960.

Hlavné funkcie:

Spracovanie OCSP požiadaviek
Generovanie odpovedí dedikovaným OCSP responderom
Kryptografické kľúče sú uložené v HSM
Dedikovaná OCSP DB
Vysoká dostupnosť a výkon

Použitie:

Efektívne overenie platnosti certifikátov
Validácia kvalifikovaných podpisov/pečatí

Funkčný opis

OCSP Responder poskytuje okamžité získanie informácie o platnosti certifikátu.

Hlavné prínosy:

Efektívnejšie overovanie platnosti elektronických podpisov/pečatí
Škálovateľnosť poskytovanej služby
Vyššia efektivita v porovnaní s CRL

Oblasti využitia:

Online informácia pre všetky spoliehajúce sa strany

4. TSA modul

Technická špecifikácia

Funkčný opis

TSA poskytuje službu kvalifikovanej časovej pečiatky podľa RFC 3161.

Hlavné funkcie:

Vyhotovovanie elektronických časových pečiatok
Kryptografické kľúče a certifikáty na podpisovanie uložené v HSM
Napojenie na presný zdroj svetového času

Použitie:

Garancia existencie elektronického dokumentu v čase
Použitie v bankách, súdnictve, verejnej správe

Časová pečiatka garantuje, že elektronický dokument alebo jeho podpis existovali v konkrétnom čase.

Hlavné prínosy:

Podpora dlhodobej overiteľnosti podpisu/pečate
Vyššia dôveryhodnosť elektronického podpisu/pečate

Oblasti využitia:

Banky
eGovernment
Archivácia elektronických podpisov

5. Audit & Compliance

Technická špecifikácia

Audit modul zabezpečuje kompletnú evidenciu všetkých činností v systéme.

Hlavné funkcie:

Logovanie operácií
Generovanie auditných správ
Export pre audítorov
Splnenie ETSI EN 319 401/411/421

Použitie:

Podklady pre eIDAS a ETSI audity
Interné bezpečnostné audity
Podpora compliance procesov

Funkčný opis

Audit modul zvyšuje transparentnosť a dôveryhodnosť prevádzky SWACA.

Hlavné prínosy:

Preukázateľnosť a zodpovednosť
Jednoduchšia príprava na audity
Plnenie legislatívnych požiadaviek

Oblasti využitia:

Poskytovatelia dôveryhodných služieb
Banky
Štátna správa

6. Používateľské portály

Technická špecifikácia

Portály pre používateľov na rôzne činnosti vykonávané počas životného cyklu certifikátu.

Hlavné funkcie:

Webové rozhranie pre vytváranie žiadosti o vydanie certifikátu
Samoobslužná správa platnosti certifikátov
Vyhľadávanie vydaných certifikátov
Vzdialené vydávanie certifikátov
Kontrola stavu čerpania časových pečiatok

Použitie:

Jednoduché sprístupnenie vybraných služieb koncovým používateľom

Funkčný opis

Portály sprístupňujú vybrané služby koncovým používateľom.

Hlavné prínosy:

Pohodlie pre používateľov
Rýchlejšie procesy
Zníženie nákladov na podporu
Zvyšuje komfort používateľov a znižuje administratívnu záťaž.

Oblasti využitia:

Veľké podniky
Banky a poisťovne
Verejná správa a univerzity

7. RA Client

Technická špecifikácia

RA Client je softvérová aplikácia pre pracovníkov registračnej autority, ktorá umožňuje spracovanie žiadostí o vydanie certifikátov.

Hlavné funkcie:

Funkčný opis

RA klient je praktický nástroj, ktorý umožňuje pracovníkom registračnej autority efektívne a bezpečne vydávať certifikáty.

Hlavné prínosy:

Viacfaktorová autentifikácia pracovníka RA
Príprava a podanie žiadostí o certifikát pracovníkom RA
Spracovanie osobných údajov žiadateľa
Bezpečná výmena údajov so SWACA
Integrácia s vybranými QSCD zariadeniami
Overenie identity žiadateľa prostredníctvom eID

Použitie:

Mobilné a externé registračné pracoviská QTSP
Zákaznícke pobočky bánk, poisťovní, telekomunikačných spoločností

Jednoduché používanie
Urýchlenie registračných procesov
Zníženie chybovosti a zvýšenie dôveryhodnosti

Oblasti využitia:

Externé RA QTSP
Banky a poisťovne
Telekomunikačné spoločnosti
Štátna a verejná správa

8. PKI klient

Technická špecifikácia

PKI klient je softvérová aplikácia pre koncové pracovné stanice. Poskytuje používateľom rozhranie na správu.

Hlavné funkcie:

Správa certifikátov na čipových kartách používateľov
Integrácia s OS a aplikáciami (Windows logon, VPN, e-mail)
Komunikácia s PKI serverom na spracovanie žiadostí
Vydanie následného certifikátu priamo z pracovnej stanice
Obnova certifikátu v prípade poškodenia čipovej karty, či straty
Upozornenia na exspiráciu certifikátov
Prehľad platných certifikátov

Použitie:

Počítače koncových používateľov v organizáciách
Správa klientskych certifikátov bez zásahu administrátora

Funkčný opis

PKI klient je nástroj pre koncových používateľov, ktorý zabezpečuje jednoduchý a bezpečný prístup k certifikátom cez komunikáciu s PKI serverom.

Hlavné prínosy:

Zníženie zaťaženia IT podpory
Zvýšenie bezpečnosti
Zjednodušenie práce s certifikátmi

Oblasti využitia:

Firemné prostredia
Verejná správa
Banky, poisťovne, telekomunikácie

9. PKI server

Technická špecifikácia

PKI server je serverový komponent v rámci SWACA, ktorý sprostredkúva komunikáciu medzi PKI klientom a systémom SWACA.

Hlavné funkcie:

Centrálny serverový komponent pre jednotlivé inštancie aplikácie PKI klient
Bezpečné prepojenie so systémom SWACA
Centralizovaná správa kryptografických algoritmov
Integrácia s MS AD

Použitie:

Manažment životného cyklu certifikátov v rámci organizácie

Funkčný opis

PKI server je centrálna súčasť PKI infraštruktúry, ktorá umožňuje jednoduché a bezpečné prevydávanie a obnovu certifikátov používateľov.

Hlavné prínosy:

Zjednodušenie procesov pre používateľov
Bezpečná komunikácia so systémom SWACA
Zjednodušenie zavedenia PKI vo veľkých organizáciách

Oblasti využitia:

Veľké a stredné organizácie
Banky a poisťovne
Štátna a verejná správa

10. CKAS server

Technická špecifikácia

CKAS server vykonáva bezpečné zálohovanie a obnovu šifrovacích kľúčov používateľov.

Hlavné funkcie:

Bezpečná záloha a obnova šifrovacích kľúčov
Podpora politiky uchovávania a obnovy kľúčov
Audit všetkých operácií

Použitie:

Funkčný opis

CKAS server je kľúčový komponent pre organizácie, ktoré používajú šifrovanie prostredníctvom certifikátov a potrebujú mať prístup k dátam aj po poškodení či strate certifikátu.

Hlavné prínosy:

Garancia možnosti dešifrovať staršie údaje aj po viacerých rokoch
Bezpečná obnova certifikátov

Zabezpečenie dlhodobého prístupu k šifrovaným dátam
Zabezpečenie kontinuity e-mailovej komunikácie (S/MIME) aj po skončení platnosti použitých šifrovacích certifikátov, ich strate a pod.
Nasadenie v prostrediach s požiadavkou na prístup k historickým dátam

bez kompromitácie kľúčov
Integrácia s HSM zákazníka
Splnenie compliance požiadaviek

Oblasti využitia:

Veľké a stredné organizácie
Banky a poisťovne
eGovernment

11. Disig Charon

Technická špecifikácia

Jednosmerný prenos dát medzi galvanicky oddelenými sieťami.

Hlavné funkcie:

Kompletné hardvérové a softvérové riešenie pre galvanické oddelenie sietí
Jednosmerné prepojenie sietí na báze „air gap" t. j. bez existencie fyzického spoja
Jednosmernosť prenosu zaručená na najnižšej vrstve ISO/OSI modelu
Striktná kontrola integrity a obsahová validácia prenášaných dát
Rozšíriteľnosť o podporu pre ľubovoľný typ prenášaných binárnych alebo textových dátových formátov
Prenosy realizované autonómne v plánovanom čase, alebo iniciované prijatím požiadavky na integračnom rozhraní
Administrácia cez aplikáciu s prehľadným grafickým používateľským rozhraním
Vývoj v zmysle požiadaviek Common Criteria (ISO/IEC 15408)

Použitie:

Ochrana CA infraštruktúry
Bezpečný prenos dát

Funkčný opis

Systém Disig Charon predstavuje jedinečnú kombináciu hardvérových a softvérových komponentov pre fyzické oddelenie počítačových sietí s rôznym stupňom utajenia.

Hlavné prínosy:

Maximálna bezpečnosť
Univerzálne použitie aj mimo PKI
Plnenie požiadaviek pre kritickú infraštruktúru

Oblasti využitia:

Národné CA
Silové rezorty
Energetika, telekomunikácie
Priemyselné systémy

Izolácia kritických systémov

12. Disig Web Signer

Technická špecifikácia

Webové riešenie pre kvalifikovaný elektronický podpis a pečať.

Hlavné funkcie:

Vyhotovovanie kvalifikovaného elektronického podpisu a pečate vo webovom prehliadači a na mobilnom zariadení
Podpora eID a všetkých QSCD zariadení s dostupným CSP alebo PKCS#11 rozhraním
Podpora eID a ďalších QSCD zariadení s bezkontaktným NFC rozhraním
Podpora pre remote signing

Použitie:

Integrácia kvalifikovaného elektronického podpisu a pečate do ľubovoľnej webovej stránky, portálu alebo mobilnej aplikácie

Funkčný opis

Web Signer umožňuje podpisovať na PC a na mobilných zariadeniach.

Hlavné prínosy:

Pohodlie pre používateľov
Dostupnosť odkiaľkoľvek
Vysoká bezpečnosť

Oblasti využitia:

Banky a poisťovne
Manažéri v teréne
Služby eGovernmentu

13. Disig QES Signer

Technická špecifikácia

Serverové riešenie pre kvalifikovaný elektronický podpis a pečať.

Hlavné funkcie:

Aplikácia na automatické vyhotovovanie a overovanie kvalifikovaného elektronického podpisu a pečate

Funkčný opis

Aplikácia Disig QES Signer umožňuje automatizovaným systémom vytvárať a overovať kvalifikovaný elektronický podpis a pečať v zmysle európskeho Nariadenia eIDAS a platnej slovenskej legislatívy.

Hlavné prínosy:

Pokročilé integračné rozhranie (SOAP) umožňujúce integráciu do firemných procesov
Vysoká škálovateľnosť
Podpora podpisovania a overovania širokého spektra formátov dokumentov
Podpora širokého spektra formátov elektronického podpisu (CAdES, XAdES, PAdES a ďalšie)

Použitie:

Backend pre špecializované portály

Škálovateľné serverové podpisovanie
Integrácia cez API
Podpora širokého spektra formátov dokumentov a podpisov

Oblasti využitia:

eGovernment portály
Bankové a poisťovacie IS
Firemné aplikácie

14. Disig QES Portal

Technická špecifikácia

Portálové riešenie pre kvalifikovaný elektronický podpis a pečať.

Hlavné funkcie:

Jednoduché REST rozhranie pre integrátorov
Možnosť prispôsobenia rozhrania a vzhľadu podľa požiadaviek zákazníka
Podpora podpisovania a overovania širokého spektra formátov dokumentov
Jadro systému tvoria aplikácie Disig QES Signer a Disig Web Signer

Použitie:

Podpisovanie zmlúv a formulárov
Overovanie vyhotovených podpisov a pečatí

Funkčný opis

QES Portal je jednoduchý a univerzálny portál na podpisovanie a overovanie.

Hlavné prínosy:

Centrálny komponent na podpisovanie a validáciu
Prívetivé používateľské rozhranie
Plne funkčné na PC a na mobilných zariadeniach

Oblasti využitia:

eGovernment
Banky a poisťovne
Korporácie

15. Disig Enterprise Signer

Technická špecifikácia

Portálové riešenie pre elektronické podpisovanie dokumentov medzi partnermi.

Hlavné funkcie:

Prispôsobiteľný workflow podporujúci komplexné riadenie a správu podpisového procesu
Podpora dokumentových šablón s možnosťou automatizovaného alebo manuálneho vkladania údajov pri odosielaní dokumentu na podpis
Zasielanie emailových notifikácií o zásadných udalostiach v systéme s URL linkami na vykonanie zodpovedajúcej akcie nad dokumentom
Okamžité sprístupnenie finálneho podpísaného dokumentu všetkým participujúcim stranám s overením el. podpisov

Použitie:

Podpisovanie dokumentov medzi viacerými stranami (typicky uzatváranie zmlúv a dohôd)
Integrácia do back-office
Zákaznícke pobočky bánk, poisťovní, telekomunikačných spoločností

Funkčný opis

Enterprise Signer zefektívňuje podpisovanie elektronických dokumentov viacerými stranami

Hlavné prínosy:

Úspora času a nákladov
Automatizácia
Spoľahlivá integrácia

Oblasti využitia:

Banky a poisťovne
Veľké korporácie
Poskytovatelia služieb

16. Disig eArchive

Technická špecifikácia

Zabezpečuje dlhodobú overiteľnosť elektronických podpisov/pečatí.

Hlavné funkcie:

Funkčný opis

eArchive zabezpečuje dlhodobú overiteľnosť elektronických podpisov/pečatí.

Hlavné prínosy:

Jednoduchá integrácia s existujúcim DMS organizácie
Úplne transparentné riešenie pre koncových používateľov DMS
Archivácia širokého spektra formátov dokumentov a elektronických podpisov

Použitie:

Archivácia elektronických podpisov
Štátne a podnikové archívy

Legislatívny súlad
Zníženie nákladov
Bezpečné uchovávanie nevyhnutných údajov k overeniu elektronického podpisu/pečate

Oblasti využitia:

Banky
Verejná správa
Prostredia vyžadujúce dlhodobú overiteľnosť podpisov

17. Disig Remote Signing

Technická špecifikácia

Vyhotovovanie kvalifikovaného elektronického podpisu na diaľku.

Hlavné funkcie:

Vyhotovovanie kvalifikovaného elektronického podpisu na mobilnom zariadení
Bezpečné uloženie a centralizovaný manažment kryptografických kľúčov
Autentizácia a autorizácia viacfaktorovým systémom využívajúcim mobilné zariadenie so SE (Secure Element) alebo externé hardvérové zariadenie
Integrácia so systémom certifikačnej autority pre automatickú správu certifikátov
Overenie totožnosti používateľa s eID kartou na úrovni zabezpečenia „vysoká“
Na prácu s kľúčmi využíva QSCD zariadenie s CC EAL 4+ certifikáciou

Použitie:

Vytváranie kvalifikovaného elektronického podpisu bez QSCD zariadenia vo vlastníctve používateľa

Funkčný opis

Disig Remote Signing umožňuje podpisovať dokumenty bez nutnosti vlastniť QSCD zariadenie

Hlavné prínosy:

Flexibilita a mobilita
Nižšie náklady na správu QSCD u používateľa

Oblasti využitia:

eGovernment
Banky a poisťovne
Verejná správa

18. Disig Validation Service

Technická špecifikácia

Disig Validation Service je serverový komponent na overovanie platnosti elektronických podpisov a pečatí v súlade s nariadením eIDAS.

Hlavné funkcie:

validácia podpisov a pečatí vo formátoch CAdES, XAdES, PAdES
kontrola platnosti certifikátov prostredníctvom OCSP a CRL
využívanie európskeho zoznamu dôveryhodných služieb (EU LOTL) resp. národných TSL
generovanie validačných protokolov
integračné rozhranie založené na SOAP API

Použitie:

kvalifikovaná služba validácie kvalifikovaných elektronických podpisov/pečatí
zaručená konverzia elektronických dokumentov v zmysle zákona č. 305/2013

Funkčný opis

Disig Validation Service je riešenie, ktoré zabezpečuje overovanie platnosti elektronických podpisov a pečatí.

Hlavné prínosy:

podpora TSP poskytujúcich kvalifikovanú službu validácie podpisov/pečatí
detailný a prehľadný report s výsledkom validácie

Oblasti využitia:

eGovernment
finančný sektor
korporácie

Manažérske zhrnutie SWACA 3.0

SWACA 3.0 je strategickým produktom spoločnosti Disig, a.s., ktorý poskytuje komplexné riešenie pre správu PKI infraštruktúry, dôveryhodné služby a elektronický podpis. Je v súlade s európskym nariadením eIDAS, národnou legislatívou a spĺňa všetky regulačné a bezpečnostné požiadavky.

Hlavnými prínosmi sú bezpečnosť, auditovateľnosť, modularita a škálovateľnosť, ktoré umožňujú nasadenie od malých CA až po národné projekty. SWACA sa dá flexibilne rozširovať o ďalšie moduly, ktoré pridávajú hodnotu pre rôzne sektory (banky, poisťovne, verejná správa, kritická infraštruktúra).

- Bezpečnosť a dôvera – integrácia s certifikovanými HSM zariadeniami, podpora ISO 27001/22301/27701.
- Súlad s legislatívou – zhoda s eIDAS a normami ETSI, pripravenosť na audity NBÚ a ENISA.
- Modularita a flexibilita – možnosť nasadiť len požadované komponenty, rozšíriteľnosť o doplnkové moduly.
- Škálovateľnosť – vhodné pre malé podnikové CA aj pre rozsiahle národné projekty a kritickú infraštruktúru.
- Efektivita a úspory – znižovanie nákladov na správu certifikátov, automatizácia procesov, samoobslužné portály pre používateľov.
- Dlhodobá udržateľnosť – podpora dlhodobej archivácie.

SWACA prináša organizáciám zvýšenú efektivitu, zníženie rizík a dlhodobú udržateľnosť procesov a umožňuje im bezpečne digitalizovať procesy, posilňuje dôveryhodnosť elektronickej komunikácie a podporuje inovácie v oblasti eGovernmentu, finančného sektora aj podnikovej sféry.

Disig a.s.,
Galvaniho 17/C,
821 04 Bratislava
Tel: +421 (0)2 208 50 140
www.disig.sk

Spoločnosť Disig a.s. si vyhradzuje právo úprav, korektúr a/alebo vylepšení informácií, produktov a programov popísaných v tomto materiáli.