I. PREDMET ŽIADOSTI

Akceptovať okrem kvalifikovaného elektronického podpisu (ďalej len „KEP“) aj zdokonalený elektronický podpis založený na kvalifikovanom certifikáte (ďalej len „AdES-QC“)?

II. APLIKOVANÉ PRÁVNE PREDPISY

Podľa čl. 13 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie (EÚ) č. 910/2014“), bez toho, aby bol dotknutý odsek 2, sú poskytovatelia dôveryhodných služieb zodpovední za škodu, ktorú spôsobia úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že nesplnia svoje povinnosti podľa tohto nariadenia.

Dôkazné bremeno týkajúce sa preukázania úmyslu alebo nedbanlivosti nekvalifikovaného poskytovateľa dôveryhodných služieb spočíva na fyzickej alebo právnickej osobe, ktorá žiada o náhradu škody uvedenej v prvom pododseku.

V prípade kvalifikovaného poskytovateľa dôveryhodných služieb sa škoda uvedená v prvom pododseku považuje za spôsobenú úmyselne alebo z nedbanlivosti, pokiaľ tento kvalifikovaný poskytovateľ dôveryhodných služieb nepreukáže opak.

Podľa odôvodnenia 21 nariadenia(EÚ) č. 910/2014, … Predovšetkým by sa nemalo vzťahovať na poskytovanie služieb, ktoré sa používajú výhradne v uzatvorených systémoch medzi vymedzenými skupinami účastníkov a ktoré **nemajú** žiaden vplyv na tretie **strany**. Požiadavky tohto nariadenia by sa napríklad nemali týkať systémov, ktoré zriadili podniky alebo orgány verejnej správy na riadenie vnútorných postupov a v rámci ktorých sa využívajú dôveryhodné služby. Požiadavky tohto nariadenia by mali spĺňať len dôveryhodné služby **poskytované verejnosti**, ktoré **majú vplyv** na tretie **strany**. …

Podľa čl. 27 ods. 2 nariadenia(EÚ) č. 910/2014, ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, **vyžaduje zdokonalený elektronický podpis založený na kvalifikovanom certifikáte**, uznáva tento členský štát **zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte** a kvalifikované elektronické podpisy, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.

Podľa čl. 2 ods. 1 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 z 8. septembra 2015, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (ďalej len „vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506“), členské štáty vyžadujúce zdokonalený elektronický podpis alebo **zdokonalený elektronický podpis založený na kvalifikovanom certifikáte**, ako sa ustanovuje v článku 27 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, **uznajú iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 tohto rozhodnutia**, za predpokladu, že členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkne iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie.

Podľa čl. 2 ods. 2 písm. c) bod 5 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 ak je zdokonalený elektronický podpis vytvorený pomocou **zariadenia na vytvorenie kvalifikovaného elektronického podpisu**, použitie každého takého zariadenia sa jasne oznámilo spoliehajúcej sa strane.

Podľa čl. 3 ods. 11 nariadenia (EÚ) č. 910/2014, „zdokonalený elektronický podpis“ je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26.

Podľa čl. 26 nariadenia (EÚ) č. 910/2014, zdokonalený elektronický podpis musí spĺňať tieto požiadavky:

a) je jedinečne spojený s podpisovateľom;
b) umožňuje určenie totožnosti podpisovateľa;
c) je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou, a
d) je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.

Podľa čl. 3 ods. 12 nariadenia (EÚ) č. 910/2014, „kvalifikovaný elektronický podpis" je zdokonalený elektronický podpis vyhotovený s **použitím zariadenia na vyhotovenie kvalifikovaného elektronického podpisu** a založený na kvalifikovanom certifikáte pre elektronické podpisy.

Podľa čl. 29 ods. 1 nariadenia (EÚ) č. 910/2014, zariadenia na vyhotovenie kvalifikovaných elektronických podpisov **musia** spĺňať požiadavky stanovené v prílohe II.

Podľa čl. 30 ods. 1 nariadenia (EÚ) č. 910/2014, zhodu zariadení na vyhotovenie kvalifikovaných elektronických podpisov s požiadavkami stanovenými v prílohe II certifikujú príslušné verejné alebo súkromné subjekty určené členskými štátmi.

Podľa čl. 30 ods. 3 nariadenia (EÚ) č. 910/2014, certifikácia uvedená v odseku 1 je založená na:

a) procese hodnotenia bezpečnosti, ktorý sa vykoná v súlade s niektorou z noriem posudzovania bezpečnosti produktov informačných technológií zaradených do zoznamu vypracovaného v súlade s druhým pododsekom, alebo
b) inom procese ako procese uvedenom v písmene a), ak sa v rámci neho používajú porovnateľné úrovne bezpečnosti a ak verejný alebo súkromný subjekt uvedený v odseku 1 tento proces oznámi Komisii. Tento proces možno použiť, len ak neexistujú normy uvedené v písmene a) alebo ak prebieha proces hodnotenia bezpečnosti uvedený v písmene a).

III. METODICKÉ USMERNENIE

Legislatíva EÚ stanovuje pre KEP, akú **minimálnu** úroveň bezpečnosti musia splniť použité procesy a prostriedky na vyhotovenie KEP, čím osoba uvedená v KEP, v kvalifikovanom certifikáte, **nemôže poprieť autorizovanie** dokumentu pomocou **KEP**, keďže museli byť použité komponenty dopredu preverené na splnenie tejto nevyhnutnej úrovne bezpečnosti (napr. čl. 3 ods. 12, čl. 29 ods. 1 a čl. 30 ods. 1 nariadenia (EÚ) č. 910/2014).

Legislatíva EÚ nedefinuje pre AdES-QC, akú minimálnu úroveň bezpečnosti by mali prostriedky na vyhotovenie AdES-QC spĺňať, pričom zavádza ďalšiu povinnosť uznať aj iné AdES-QC v čl. 27 ods. 2 nariadenia (EÚ) č. 910/2014 a čl. 2 ods. 1 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506, akými sú napr. AdES-QC vyhotovené na zariadení na vyhotovenie kvalifikovaného elektronického podpisu (**QSCD**) v inom formáte podpisu než uvedenom v prílohe vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506, čím umožňuje osobe autorizujúcej dokument s AdES-QC sa pokúsiť **poprieť**, že dokument autorizovala, čo spoliehajúca strana dodatočne buď preukáže alebo nie. V prípade sporu je potrebné pri AdES-QC **dodatočné posúdenie**, či prostriedok použitý na vyhotovenie AdES-QC a použité postupy spoliehajúcej strane umožnia odvrátiť popretie vyhotovenia.

Ak je dokument autorizovaný AdES- QC, spoliehajúca sa strana nemusí mať istotu, či boli dodržané aspoň odporúčané bezpečnostné požiadavky, a teda ak nemusí, nebude akceptovať AdES-QC. Pri použití AdES-QC nemusí byť odhalené vydanie kvalifikovaného certifikátu pre vyhotovenie AdES-QC na kľúč generovaný v čipe so závažnou bezpečnostnou zraniteľnosťou

ROCA RSA algoritmu, napr. na čipe eID s ukončenou certifikáciou, alebo generovaný, či uložený iným nebezpečným spôsobom, keďže takú kontrolu legislatíva EÚ nevyžaduje pre AdES-QC, čo ak by občan ako spoliehajúca sa strana zistil, napr. po medializovanom prepuknutí takéhoto úmyselného konania vedúceho k závažným incidentom, mohol by stratiť dôveru v akékoľvek elektronické služby poskytované a garantované štátom.

Úrad odporúča zvážiť negatíva, ktoré by nastali v dôsledku zníženia úrovne bezpečnosti z KEP na AdES-QC.

Požiadavky definované legislatívou na KEP garantujú dodržanie presných postupov pri vydaní a aj validovaní KEP, zatiaľ čo AdES-QC v prípade popretia zo strany podpisovateľa alebo zo strany spoliehajúcej sa strany, je potrebné dodatočne posúdiť, keďže legislatíva nedefinuje povinné minimálne požiadavky. Pre subjekty verejného sektora je dôležité zhodnotiť agendy a určiť, v ktorej ich agende nepotrebujú KEP, teda nevadí, ak by neskoršie mohlo dôjsť k pokusu popretiu autorizácie osobou uvedenou v elektronickom podpise a dodatočné preverenie procesov vyhotovenia AdES-QC nepovažujú za potrebné, keďže si napr. spätne potrebné údaje a súhlas osoby vedia v danej agende preveriť.

Akceptovanie AdES-QC úradom:

- Úrad neidentifikoval agendy, v ktorých by postačoval AdES-QC.
- Úrad validuje autorizované prílohy prijaté elektronickou poštou alebo z ústredného portálu verejnej správy (ďalej len „ÚPVS“) v aplikácii QES (aplikácia úradu), kde je uvedený typ autorizácie vo validačnej správe:
  - kvalifikovaný elektronický podpis/pečať (KEP - QES),
  - zdokonalený elektronický podpis/pečať založený na kvalifikovanom certifikáte (AdES-QC),
  - zdokonalený elektronický podpis/pečať (AdES),
  - elektronický podpis (ES) a
  - kvalifikovaná elektronická časová pečiatka.
- Aplikácia QES (aplikácia úradu) vie vyhotoviť KEP a aj AdES-QC. Pre vyhotovenie AdES-QC je možné použiť súborové úložisko podpisového kľúča a kvalifikovaného certifikátu (*.p12 alebo *.pfx) alebo MS Windows úložisko kľúčov s certifikátmi a aj čipové karty.

Ak bude subjekt verejného sektora akceptovať AdES-QC, keďže postupy na vyhotovenie AdES-QC nevyžadujú dopredu preukázanie splnenie minimálnych podmienok na vyhotovenie AdES-QC, subjekt verejného sektora preberá zodpovednosť v prípade chybného či nevhodného rozhodnutia občana použiť AdES-QC, kedy si subjekt verejného sektora mal dodatočne preveriť, napr. potvrdením splnenia minimálnych bezpečnostných požiadaviek vyhotoviteľom AdES-QC. Občan a aj subjekt verejného sektora by sa mohli dostať do situácie, kedy napríklad akceptujú AdES-QC, ale AdES-QC už nemôžu predložiť inému subjektu, ktorý neakceptuje AdES-QC, keďže akceptovanie AdES-QC nie je povinné vzhľadom na čl. 27 ods. 2 nariadenia (EÚ) č. 910/2014 a čl. 2 ods. 1 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506 a z dôvodu nedefinovania minimálnej úroveň bezpečnosti, o ktorej skutočnej úrovni sa spoliehajúca sa strana nemá možnosť uistiť (ak nejde o uzavretý systém, v ktorom si definujú vlastné pravidlá), a tak jej zostáva akceptovať AdES-QC len v takej agende, kde akceptuje aj chybné údaje a vie si ich neskôr dodatočne preveriť.

Uvádzame hlavné rozdiely medzi KEP a AdES-QC z pohľadu možného zneužitia:

- KEP (QES) - musí mať splnené minimálne podmienky legislatívy EÚ, na čo dohliada orgán dohľadu v každej krajine EÚ (v Slovenskej republike úrad), čím je povinnosť akceptovať KEP v celej EÚ subjektom verejného sektora podľa čl. 27 ods. 3 nariadenia (EÚ) č. 910/2014.

- AdES-QC - legislatíva EÚ nedefinuje minimálne bezpečnostné úrovne pre prostriedok na vyhotovenie AdES-QC, čím môže dôjsť k jeho klonovaniu, alebo použitiu inou osobou bez vedomia osoby uvedenej v kvalifikovanom certifikáte.
- AdES - okrem nedostatkov AdES-QC, certifikát nie je kvalifikovaný, a teda legislatívou EÚ nie je stanovený jednotný proces garantujúci správnosť údajov v certifikáte. Certifikát môže vydať ktokoľvek, aj sama osoba si ho môže vydať pre seba.
- ES - okrem nedostatkov AdES, formát podpisu nezabezpečí napr. ochranu pred substitučnými útokmi na výmenu certifikátu, a tak je možné zmeniť údaje o podpisovateľovi, vydavateľovi, a tým aj o platnosti certifikátu v ES.

Ak dotknutý subjekt akceptuje AdES-QC namiesto KEP, musí akceptovať svoju zodpovednosť za nesprávne úkony, keďže AdES-QC umožňuje:

- odmietnuť akceptovať AdES-QC inou spoliehajúcou sa stranou akceptujúcou iba KEP podľa čl. 27 ods. 2 nariadenia (EÚ) č. 910/2014 a čl. 2 ods. 1 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1506,
- prípadné podvody, v ktorých podpis vyhotoví iná osoba než je osoba uvedená v kvalifikovanom certifikáte, čo je potrebné dodatočne preukázať, keďže pri vydaní kvalifikovaného certifikátu pre AdES-QC legislatíva EÚ nevyžaduje pri vydaní kvalifikovaného certifikátu to skontrolovať a
- osoba uvedená v kvalifikovanom certifikáte sa môže kedykoľvek pokúsiť poprieť, že by podpis AdES-QC vyhotovila, čo je potrebné dodatočne preukázať - legislatíva EÚ nevyžaduje pri vydaní kvalifikovaného certifikátu pre AdES-QC použiť prostriedok umožňujúci výhradnú kontrolu.

V aktuálne navrhovaných revíziách legislatív EÚ sa smeruje opačným smerom, než je znížiť dôveru v elektronickú komunikáciu medzi občanom a štátom požitím AdES-QC. V EÚ prevažuje cieľ dosiahnuť najvyššiu úroveň bezpečnosti pri identifikácii, autentifikácii a elektronickom podpise, čo je úroveň „vysoká“ a použitie KEP, aby osoba mohla bez obáv pristúpiť k ľubovoľnej službe vo svojej krajine, a aj v zahraničí.