MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX03V4NAO
prvotní identifikátor

odbor eGovernmentu
náměstí Hrdinů 1634/3
Praha 4
140 21

Č. j. MV- 60736-36/EG-2016

Praha 2. března 2018

Stanovisko k použití kvalifikovaných certifikátů pro autentizaci internetových stránek.

Odbor eGovernmentu Ministerstva vnitra zveřejňuje na základě žádosti kvalifikovaného poskytovatele služeb vytvářejících důvěru, stanovisko k přípustným možnostem použití kvalifikovaných certifikátů pro autentizaci internetových stránek (dále jen „QWAC“) vydaných v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“). V rámci žádosti o stanovisko, byl odbor eGovernmentu požádán o vyjádření k následujícím otázkám:

1. *Podle písm. e) přílohy IV nařízení eIDAS obsahují QWAC povinně „název domény nebo domén, které provozuje fyzická nebo právnická osoba, jíž je certifikát vydán“. Přihlédneme k definicím, ve kterých je uvedeno, že „certifikátem pro autentizaci internetových stránek (se rozumí) potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán“. Předpokládáme tedy, že žadatel o certifikát musí být schopen doložit, že je držitelem příslušné domény, příp. domén, a QTSP [kvalifikovaný poskytovatel služeb*

vytvářejících důvěru] musí mít možnost tuto skutečnost ověřit. Pokud tyto podmínky nejsou splněny, certifikát nelze vydat.

2. *Je přípustné, aby ten, komu byl QWAC vydán, použil příslušný soukromý klíč i na jiném serveru či k jinému účelu? Nebo má naopak QTSP povinnost klienta zavázat, že tak činit nebude, a to i s ohledem na povinnost stanovenou v nařízení eIDAS v čl. 24 odst. 1 písm. d) ohledně informování budoucího klienta o přesných podmínkách používání dané služby, včetně případných omezení?*
3. *Je obecně konstatováno, že úpravě QWAC je v nařízení eIDAS věnována minimální pozornost. Zejména zcela absentují požadavky na ochranu soukromého klíče. Mají orgány EU nebo Ministerstvo vnitra v tomto směru nějaké doporučení? Opět i s vazbou na povinnost stanovenou v nařízení eIDAS v čl. 24 odst. 1 písm. d).*
4. *Bohužel rovněž absentuje úprava zneplatnění QWAC, příp. pozastavení jeho platnosti. Na tyto případy lze vztáhnout obecnou povinnost pro jakýkoliv typ kvalifikovaného certifikátu uvedenou v čl. 24, odst. 3 a 4. QTSP by pak měl v Certifikační politice či ve smlouvě klienta zavázat, že jakmile se změní údaje uvedené v certifikátu, včetně změny držitele domény, dojde ke kompromitaci soukromého klíče apod., klient si u QTSP vyžádá zneplatnění QWAC a ihned jej přestane používat.*
5. *Pokud připustíme použití QWAC pro „klienta“, resp. pro navázání spojení a komunikaci dvou rozhraní, pak je nezbytné či alespoň žádoucí každou relaci opatřit kvalifikovanou elektronickou pečetí. Důvodem je skutečnost, že QWAC nejsou spojeny s takovými vlastnosti, jakými jsou prokázání původu a integrity dat, a je tedy nezbytné je zajistit jiným způsobem, tj. elektronickým podpisem nebo pečetí.*

K otázce č. 1:

Souhlasíme, že nedílnou součástí QWAC vydaného v souladu s přílohou IV. nařízení eIDAS je rovněž informace o názvu domény nebo domén, které provozuje fyzická nebo právnická osoba, jíž je certifikát vydán. Požadavek na uvedení názvu domény nebo domén

v QWAC, je výslovně stanoven v požadavcích přílohy IV. nařízení eIDAS [písm. e)]. Ve spojitosti s čl. 45 odst. 1 nařízení eIDAS („*Kvalifikované certifikáty pro autentizaci internetových stránek musí splňovat požadavky stanovené v příloze IV.*“) lze tudíž vyvodit, že pokud vydaný certifikát neobsahuje informaci o názvu domény nebo domén, které provozuje fyzická nebo právnická osoba, pak tento certifikát nesplňuje požadavky na QWAC stanovené v příloze IV. nařízení eIDAS.

V případě, kdy žadatel o certifikát není schopen doložit, že provozuje příslušnou doménu, příp. domény, nebo kvalifikovaný poskytovatel služeb vytvářejících důvěru nemůže tuto skutečnost ověřit, pak nelze QWAC tomuto žadateli vydat.

K tomuto bodu dále uvádíme, že kvalifikovaný poskytovatel služeb vytvářejících důvěru se dopustí správního deliktu, pokud vydá QWAC, který neodpovídá požadavkům nařízení eIDAS [viz § 17 odst. 4 písm. h)] zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů).

K otázce č. 2:

S ohledem na funkci certifikátů pro autentizaci internetových stránek („*potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán*“) jsme toho názoru, že není přípustné, aby příslušný soukromý klíč k veřejnému klíči uvedenému v QWAC, se používal i na jiném serveru než na serveru, pro který byl QWAC vydán (tj. pro jinou doménu, než která je uvedena v QWAC – doména je obvykle uvedena v atributu certifikátu CN [obecné jméno]). Popíral by se tak de-facto účel certifikátu, který má věrohodně spojit konkrétní doménu s konkrétním subjektem, který tuto doménu provozuje. Pomocí QWAC či EV (Extended Validation) SSL certifikátů lze zabránit

phishingu internetových stránek (uživatel internetových stránek se může díky těmto certifikátům přesvědčit, že doménu provozuje legitimní subjekt).

Dalším možným účelem použití QWAC je dle názoru odboru eGovernmentu takové použití, kdy se QWAC použije pro navázání SSL/TLS spojení, v rámci kterého se automatizovaně vyměňují data mezi dvěma rozhraními (spojení se vzájemnou autentizací). Účelem takového spojení je zejména zaručit důvěrnost vyměňovaných dat mezi koncovými body spojení spolu se vzájemnou důvěryhodnou identifikací těchto bodů vůči sobě navzájem. Použití QWAC v tomto smyslu nezajišťuje následnou integritu či původ vyměňovaných dat (data, pokud nejsou dále zabezpečena, vstupují na jednom konci spojení v otevřené podobě a rovněž na druhém konci spojení vystupují v otevřené podobě). Tj. data jsou chráněna pouze při přenosu, nikoliv následně po té, co jsou data kanálem přenesena. Použití QWAC pro navázání vzájemně autentizovaného SSL/TLS spojení připouští rovněž dokument „Security guidelines on the appropriate use of qualified website authentication certificates“ vydaný agenturou ENISA (Agentura Evropské unie pro bezpečnost sítí a informací). Výše uvedený dokument má sloužit jako podpůrný materiál, který má napomoci pochopení klíčových vlastností QWAC společně s příklady, jak v praxi těchto vlastností využít. Ze své podstaty se jedná o nezavazující materiál a je možné je nalézt na stránkách agentury ENISA: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-website-authentication-certificates. Dalším dokumentem vyslovujícím se pro možnost použití QWAC rovněž pro identifikaci klienta při navazování TLS spojení je draft technických specifikací ETSI TS 119 495 V0.0.3 (2018-01) Electronic Signatures and Infrastructures (ESI);Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU, jehož verze k veřejnému připomínkování je k dispozici zde: https://docbox.etsi.org/ESI/Open/Latest_Drafts/ts_119495v000003_for-public-review.pdf. Draft technických specifikací se týká použití kvalifikovaných certifikátů pro elektronické

pečetě a kvalifikovaných certifikátů pro autentizaci internetových stránek v rámci směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (obecně známá jako „směrnice PSD 2“). V příloze B draftu technických specifikací se připouští rovněž možnost, aby QWAC byly použity také pro identifikaci klienta v rámci TLS spojení. Vzhledem k tomu, že v praxi může dojít při implementaci možnosti použití QWAC k identifikaci klienta v rámci TLS spojení k výkladovým problémům ve spojitosti s dalšími technickými standardy, odbor eGovernmentu požádal organizaci ETSI v průběhu veřejného připomínkování draftu technických specifikací, o další informace. Před případným použitím QWAC pro autentizaci klienta v rámci TLS spojení, odbor eGovernmentu doporučuje tento účel použití zkontrolovat vůči certifikační politice pro vydávání QWAC, případně zamýšlený účel použití zkonzultovat s kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Stran informování budoucího klienta o přesných podmínkách používání dané služby, včetně případných omezení, je kvalifikovaný poskytovatel služeb vytvářejících důvěru povinen před vydáním QWAC informovat jasným a srozumitelným způsobem osobu, která žádá o vydání QWAC, o přesných podmínkách používání této služby, včetně případných omezení jejího využívání a to v souladu s odkazovaným čl. 24 odst. 2 písm. d) nařízení eIDAS. Obvykle se informace o podmínkách používání kvalifikovaných služeb vytvářejících důvěru zveřejňují v politikách kvalifikovaných služeb vytvářejících důvěru, jež jsou volně přístupné a umístěné např. na internetových stránkách poskytovatele či na jeho pracovištích. V rámci politiky vydávání QWAC pak kvalifikovaný poskytovatel specifikuje přípustné použití (účel) vydávaných QWAC. Pokud klient tyto podmínky nebo omezení nedodrží, pak se poskytovatel zříká jakékoliv odpovědnosti plynoucí z nepovoleného použití. Tzn., v případě nastalé škody plynoucí z použití QWAC v rozporu s politikou, podle které byl vydán, kvalifikovaný poskytovatel služeb vytvářejících důvěru nenese odpovědnost za škodu [vizte čl. 13 odst. 2

nařízení eIDAS a čl. 24 odst. 2 písm. d) nařízení eIDAS]. Z pohledu žadatele o vydání QWAC je tudíž klíčové posoudit, zda účel (použití) certifikátu specifikovaný v politice odpovídá zamýšleným účelům použití ze strany žadatele.

Pro úplnost je vhodné doplnit, že certifikační politiky obvykle obsahují i povinnosti pro spoléhající se strany (tj. pro subjekty, které se spoléhají na certifikáty vydané podle konkrétní politiky). Namátkou lze uvést, že spoléhající se strany si musí ověřit platnost certifikátů (a to nejen platnost koncového certifikátu, ale rovněž i platnost nadřazených certifikátů certifikační autority). Opět, pokud nastane škoda díky nedodržení povinností ze strany spoléhající se strany, kvalifikovaný poskytovatel služeb vytvářejících důvěru se zříká odpovědnosti za škodu. Z výše uvedeného je zřejmé, že obecně při výběru vhodného typu certifikátu, je nutné dbát předpokládaného použití certifikátů a podle toho vybírat konkrétní typ certifikátu. Pokud se certifikát bude používat v rozporu s definovaným účelem použití, pak se riziku úhrady za vzniklou škodu vystavuje jak držitel certifikátu, tak i spoléhající se strana.

K otázce č. 3 a 4 :

Odbor eGovernmentu je toho názoru, že držitel QWAC musí věnovat dostatečnou pozornost při ochraně příslušného soukromého klíče souvisejícího s veřejným klíčem uvedenému ve vydaném QWAC tak, aby snížil na minimum možnost zneužití tohoto soukromého klíče. Měl by tedy přijmout nezbytná technicko organizační opatření, která zabrání možnému zneužití soukromého klíče. Zavázat klienta k požadavku ochrany soukromého klíče rovněž vybízí sdružení CA/Browser Forum, které stanovuje pravidla pro vydávání SSL certifikátů (např. Domain Validation [DV], Organizational Validation [OV], Extended Validation [EV]). QWAC jsou „evropskou“ obdobou EV SSL certifikátů. Konkrétně v základních požadavcích pro vydávání a správu důvěryhodných SSL certifikátů, toto sdružení

stanovuje povinnost pro certifikační autority, aby zavázali klienta k patřičné ochraně příslušného soukromého klíče:

Protection of Private Key:

An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

Viz kapitola 9.6.3. dokumentu Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates dostupného na adrese: https://cabforum.org/baseline-requirements-documents/.

Domníváme se, že držitel QWAC by měl být smluvně zavázán, podobně jako např. držitel kvalifikovaného certifikátu pro elektronický podpis, že je jeho povinností nahlásit poskytovateli podezření na zneužití, či přímo ztrátu nebo krádež příslušného soukromého klíče. Stejně tak informování v případě, kdy se změnily údaje uvedené v QWAC. Držitel QWAC pak musí samozřejmě příslušný soukromý klíč přestat používat v případě výskytu výše uvedených okolností. Na druhou stranu pro kvalifikovaného poskytovatele platí povinnost zneplatnit jím vydaný QWAC do 24 hodin od obdržení žádosti, pokud je žádost o zneplatnění vyhodnocena jako pravá (validní). A dále poskytovat informace o platnosti nebo o zneplatnění kvalifikovaných certifikátů v souladu s nařízením eIDAS.

K otázce č. 5 :

Jak již bylo řečeno v souvislosti s odpovědí na otázku č. 2, domníváme se, že QWAC mohou být užity rovněž pro navázání SSL/TLS spojení, kdy je třeba vzájemná autentizace komunikujících bodů. QWAC by v tomto smyslu použití fungovaly jako prostředek, pomocí kterého lze důvěryhodně ověřit identitu komunikujícího bodu v první fázi navazování SSL/TLS

spojení (tzv. „handshake“). Vyměňovaná data přes toto spojení, pokud nejsou dále zabezpečena, vstupují na jednom konci SSL/TLS spojení v otevřené podobě a rovněž na druhém konci spojení vystupují ve stejné podobě jako na vstupu. Použití QWAC přenášeným datům nedává záruku původu či integrity dat poté, co jsou data spojením přenesena.

V případě, kdy je nutné zajistit původ či integritu dat, je nutné použít dalších prostředků (např. z důvodu legislativních požadavků či z důvodu bezpečnosti a průkaznosti pro třetí strany). Tímto prostředkem může být kvalifikovaná elektronická pečeť. U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena (vizte čl. 35 odst. 2 nařízení eIDAS) přičemž je vhodné doplnit, že elektronicky pečetit mohou pouze právnické osoby. Kromě kvalifikovaných elektronických pečetí lze samozřejmě využít také zaručené elektronické pečeti nebo zaručené elektronické pečeti založené na kvalifikovaných certifikátech pro elektronické pečeti. V závislosti na analýze rizik konkrétního případu užití by subjekt měl rozhodnout, jaký typ elektronické pečeti použít s ohledem na dosažení požadované úrovně bezpečnosti. Alternativně se nabízí použití i jiných prostředků a technologií.

Pokud komunikace probíhá mezi body, jež jsou spravovány fyzickými osobami, pak je možné použít pro zaručení autenticity a integrity dat kvalifikovaného elektronického podpisu, případně jeho dalších typů umožňující zaručit integritu dat (zaručený elektronický podpis, zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis), a to opět s ohledem na dosažení požadované úrovně bezpečnosti. Při použití elektronického podpisu je nutné dbát na skutečnost, že by neměla být podepisována ta data, se kterými se podepisující osoba nemá možnost seznámit. Pokud je nutné zabezpečit autenticitu a integritu strojové komunikace dat, se kterou se fyzická osoba nemá možnost seznámit, mělo by se pro zabezpečení těchto dat využít například komerčních certifikátů.

Závěrem si dovolujeme uvést, že uvedené stanovisko je toliko právním názorem odboru eGovernmentu, který není oprávněn k autoritativnímu výkladu právních předpisů. Tato kompetence náleží v konkrétním případě výlučně soudu.

Ing. Roman Vrba
ředitel

Elektronický podpis - 5.3.2018
Certifikát autora podpisu :
Jméno : Ing. Roman Vrba
Vydal : PostSignum Qualified C...
Platnost do : 2.7.2018