PODMIENKY ZRUŠENIA TLS CERTIFIKÁTU VYDANÉHO CERTIFIKAČNOU AUTORITOU CA DISIG

V prípade, že musí byť zrušený TLS certifikát koncovej entity t. j. certifikát, ktorý je možné použiť pre servery s možnosťou využitia TLS protokolu (ďalej len „certifikát“) z jedného z týchto dôvodov:

- keyCompromise (RFC 5280 CRLReason #1),
- privilegeWithdrawn (RFC 5280 CRLReason #9),
- cessationOfOperation (RFC 5280 CRLReason #5),
- affiliationChanged (RFC 5280 CRLReason #3) alebo
- superseded (RFC 5280 CRLReason #4),

musí byť koncový držiteľ informovaný o týchto možnostiach spolu s vysvetlením, kedy zvoliť jednotlivé možnosti pri žiadaní o zrušenie certifikátu.

keyCompromise

Dôvod zrušenia certifikátu **keyCompromise** MUSÍ byť použitý, keď nastane jedna alebo viacero z nasledujúcich situácií:

- prevádzkovateľ CA získa overiteľný dôkaz, že súkromný kľúč držiteľa certifikátu zodpovedajúci verejnému kľúču v certifikáte bol kompromitovaný,
- operátor CA je informovaný o preukázanej alebo overenej metóde, ktorá vystavuje súkromný kľúč predplatiteľa certifikátu kompromitácii,
- existuje jasný dôkaz, že špecifická metóda použitá na generovanie súkromného kľúča bola chybná,
- operátor CA je informovaný o preukázanej alebo overenej metóde, ktorá umožňuje jednoducho vypočítať súkromný kľúč držiteľa certifikátu na základe verejného kľúča v certifikáte (ako je napr. Debian weak key, pozri https://wiki.debian.org/TLSkeys), alebo
- držiteľ certifikátu požiada prevádzkovateľa CA o zrušenie certifikátu z tohto dôvodu, pričom rámec zrušenia je popísaný nižšie.

Uplatnenie zrušenia závisí od toho, či predplatiteľ certifikátu preukázal vlastníctvo súkromného kľúča certifikátu. Samotná žiadosť v podobe CSR nepreukazuje držbu súkromného kľúča certifikátu na účely iniciovania zrušenia.

- Ak ktokoľvek žiadajúci o zrušenie z dôvodu keyCompromise predtým preukázal alebo môže v súčasnosti preukázať vlastníctvo súkromného kľúča certifikátu, potom operátor CA MUSÍ zrušiť všetky inštancie tohto kľúča u všetkých držiteľov.

- Ak držiteľ certifikátu požiada operátora CA o zrušenie certifikátu z dôvodu keyCompromise a predtým nepreukázal a momentálne nemôže preukázať vlastníctvo priradeného súkromného kľúča tohto certifikátu, operátor CA MÔŽE zrušiť všetky certifikáty spojené s týmto držiteľom, ktoré obsahujú daný verejný kľúč. Prevádzkovateľ CA NESMIE predpokladať, že má dôkaz o kompromitácii súkromného kľúča na účely zrušenia certifikátov iným účastníkov, ale MÔŽE zablokovať vydávanie budúcich certifikátov s týmto kľúčom.

V opačnom prípade sa dôvod zrušenia keyCompromise NESMIE použiť.

privilegeWithdrawn

Dôvod zrušenia certifikátu **privilgeWithdrawn** je určený na použitie vtedy, keď došlo k porušeniu pravidiel na strane držiteľa, ktoré neviedlo ku kompromitácii súkromného kľúča, ako napríklad prípad, kedy držiteľ certifikátu poskytol zavádzajúce informácie vo svojej žiadosti o certifikát alebo nedodržal svoje záväzky podľa zmluvy alebo podmienok použitie.

Pokiaľ sa nepoužije dôvod zrušenia keyCompromise, MUSÍ sa použiť privilegeWithdrawn v prípade, keď:

- prevádzkovateľ CA získa dôkaz o zneužití certifikátu,
- prevádzkovateľ CA je upozornený na to, že držiteľ certifikátu porušil jednu alebo viacero svojich podstatných povinností vyplývajúcich zo zmluvy alebo podmienok používania,
- operátor CA je informovaný o tom, že wildcard certifikát bol použitý na overenie podvodne zavádzajúceho podriadeného plne kvalifikovaného názvu domény (FQDN),
- prevádzkovateľ CA je informovaný o podstatnej zmene informácií obsiahnutých v certifikáte,
- prevádzkovateľ CA zistí alebo je upozornený, že ktorákoľvek z informácií uvedených v certifikáte je nepresná, alebo
- operátor CA je upozornený, že pôvodná žiadosť o certifikát nebola autorizovaná a že držiteľ autorizáciu spätne neudelil.

V opačnom prípade sa dôvod zrušenia privilegeWithdrawn NESMIE použiť.

cessationOfOperation

Dôvod zrušenia certifikátu **cessationOfOperation** je určený na použitie, v prípade kedy je webová stránka s certifikátom vypnutá pred vypršaním platnosti certifikátu, alebo ak držiteľ už nevlastní alebo nekontroluje názov domény v certifikáte. Tento dôvod zrušenia sa má použiť v nasledujúcich prípadoch:

- držiteľ certifikátu už nekontroluje alebo už nie je oprávnený používať všetky názvy domén v certifikáte,

- držiteľ certifikátu už nebude používať certifikát, pretože ukončuje prevádzku svojej webovej stránky, alebo
- prevádzkovateľ CA získa informáciu o okolnosti, ktorá naznačuje, že používanie plne kvalifikovaného názvu domény alebo IP adresy v certifikáte už nie je zo zákona povolené (napr. súd zrušil registrátorovi názvu domény právo používať názov domény, príslušná licenčná zmluva alebo zmluva o službách medzi registrátorom názvu domény a žiadateľom bola ukončená alebo registrátor názvu domény nepredĺžil názov domény).

Pokiaľ sa nepoužije dôvod zrušenia keyCompromise, MUSÍ sa použiť dôvod zrušenia cessationOfOperation v prípade keď:

- držiteľ certifikátu požiadal o zrušenie certifikátu z tohto dôvodu, alebo
- operátor CA dostal overiteľný dôkaz, že držiteľ certifikátu už nekontroluje alebo už nie je oprávnený používať všetky názvy domén v certifikáte.

V opačnom prípade sa dôvod zrušenia cessationOfOperation NESMIE použiť.

affiliationChanged

Dôvod zrušenia certifikátu **affiliationChanged** je určený na to, aby sa používal na označenie toho, že meno subjektu alebo iné informácie o identite subjektu v certifikáte sa zmenili, ale nie je dôvod domnievať sa, že bol ohrozený súkromný kľúč certifikátu.

Pokiaľ sa nepoužije dôvod zrušenia keyCompromise, MUSÍ sa použiť dôvod affiliationChanged v prípade, keď:

- držiteľ certifikátu požiadal o zrušenie certifikátu z tohto dôvodu, alebo
- operátor CA vydal nový certifikát z dôvodu zmien v informáciách o subjekte certifikátu a CA nenahradila certifikát z iných dôvodov: keyCompromise, superseded, cessationOfOperation alebo privilegeWithdrawn.

V opačnom prípade sa dôvod zrušenia affiliationChanged NESMIE použiť.

superseded

Dôvod zrušenia certifikátu **superseded** sa použije v prípade, keď:

- držiteľ certifikátu požiadal o nový certifikát, ktorý nahradí existujúci certifikátu; alebo
- prevádzkovateľ CA získa hodnoverné dôkazy o tom, že na overenie autorizácie domény alebo kontroly pre akýkoľvek plne kvalifikovaný názov domény alebo IP adresu v certifikáte sa nedá spoľahnúť, alebo
- operátor CA zrušil certifikát z dôvodov súladu, napríklad certifikát nie je v súlade s politikou Mozilla Root Store Policy, s požiadavkami CA/Browser Forum's Baseline Requirements alebo s CP alebo CPS vydávajúcej CA.

Pokiaľ sa nepoužije dôvod zrušenia keyCompromise, MUSÍ byť použitý dôvod supeseded v prípade, keď:

- držiteľ certifikátu požiadal o zrušenie certifikátu z udaním tohto dôvodu, alebo
- prevádzkovateľ certifikačnej autority zrušil certifikát z dôvodu iných problémov s autorizáciou domény alebo s dodržiavaním predpisov, ako sú tie, ktoré súvisia s dôvodom keyCompromise alebo priorityWithdrawn.

V opačnom prípade sa dôvod zrušenia superseded NESMIE použiť.

Ak pri analýze dôvodov zrušenia zistíte, že dôvody napĺňajú niektorú z vyššie uvedených prípadov, tak žiadosť o zrušenie musí by v prípade, že žiadate o zrušenie TLS certifikátu bez osobnej účasti, podaná prostredníctvom formulára žiadosti na zrušenie, ktorý je dostupný tu: https://dsrv.disig.sk/download/forms/tls_revoke_form.pdf

V prípade, že pri analýze dôvodov zrušenia zistíte, že nie sú naplnené charakteristiky vyššie uvedených prípadov, tak na zrušenie postačuje zaslanie e-mailovej požiadavky s uvedením sériového čísla TLS certifikátu a hesla na zrušenie na e-mailovú adresu radisig@disig.sk