Informace pro vývojáře aplikací – září 2020

Datum: 18. 8.2020
Verze: 1.1.
Klasifikace: veřejný dokument

1 Anotace změn

1. V souladu s všeobecně doporučovanými postupy zavádí ISDS další bezpečnostní úpravy konfigurace webového serveru. Toto opatření může mít dopad na některé staré, neaktualizované aplikace, které se připojují k ISDS.
2. Zavádí se nová událost doručenky – informace o doručení fikcí ve schránce, v níž nebyl po dobu 10 dnů od dodání žádný uživatel.

2 Harmonogram změny

V prostředí veřejného testu ISDS bude změna nasazena **6.9.2020**. Na produkčním ISDS bude změna nasazena pravděpodobně v **prosinci 2020**.

3 Popis změn

3.1 Změna pořadí šifrovacích sad

Webový server při výběru šifrovací sady vyjednávané s klientem aplikuje preferenční pořadí a upřednostňuje silné šifrovací sady. Akceptuje však ještě také zastaralé, nedostatečně bezpečné a slabé šifrovací sady s HMAC SHA-1.

Na všech rozhraních bude (postupně) vypnuta podpora těchto šifrovací sad:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)

Pro ověření funkčnosti se stačí po odstávce 6.9.2020 přihlásit do nějaké schránky v testovacím prostředí ISDS. Pro naprostou většinu aplikací se nic nezmění, stejně tak jako pro uživatele webové aplikace Klientský portál ISDS.

3.2 Doručení fikcí do schránky bez uživatelů

Zákon č. 300/2008 Sb. o el. úkonech a autorizované konverzi dokumentů jasně stanovuje v § 17 odst. 4, že veřejná datová zpráva je doručena desátým dnem po dodání, pokud se dříve nepřihlásila do schránky osoba s právem čtení této zprávy. Výjimku tvoří datové zprávy, které odesílající OVM označilo příznakem „Nedoručovat fikcí“.

Datová zpráva, doručená tímto způsobem, je ve stavu „Doručeno fikcí (5)“, odlišném od stavu, kdy se do schránky někdo přihlásil a mohl si zprávu stáhnout a přečíst – „Doručeno přihlášením (6)“. Na tomto principu se úpravou nic nemění, doručení fikcí bude i nadále uplatňováno.

Na základě stanoviska Nejvyššího správního soudu se však správce ISDS rozhodl poskytovat informace o situaci, kdy do schránky reálně nikdo neměl přístup. Nově tak budou rozlišeny dvě situace při doručení zprávy fikcí:

1. Do schránky se nikdo nepřihlásil, i když mohl;
2. Do schránky se nikdo nepřihlásil, protože nemohl (zjednodušeně: ve schránce po celou dobu 10 dnů od dodání do doručení fikcí neexistoval žádný uživatel).

Datová zpráva podle bodu 2 bude mít v doručence **novou událost E6**, následující za událostí E2 – doručení fikcí. Událost E6 (na portále, ve WS i v PDF doručence) má popis:

> *EV6: V datové schránce adresáta nebyla v době od okamžiku dodání zprávy do okamžiku doručení zprávy fikcí zavedena žádná osoba s oprávněním přistupovat do datové schránky.*

Obrázek 1 – nová událost E6 v doručence zobrazené v portálu

3.2.1 Webové služby

Veřejné webové služby **GetDeliveryInfo** a **GetSignedDeliveryInfo** vracejí pole událostí (element `dmEvents`) vztahujících se k doručování zprávy, obsahující v každém záznamu čas události a popis události. Pro zprávu jako výše vypadá výstup:

…

```
<q:dmDeliveryTime>2020-07-17T10:20:13.463+02:00</q:dmDeliveryTime>
<q:dmAcceptanceTime>2020-07-27T10:20:13.000+02:00</q:dmAcceptanceTime>
<q:dmMessageStatus>5</q:dmMessageStatus>
<q:dmEvents>
   <q:dmEvent>
      <q:dmEventTime>2020-07-17T10:20:13.260+02:00</q:dmEventTime>
```

```
                  <q:dmEventDescr>EV0: Datová zpráva byla podána.</q:dmEventDescr>
               </q:dmEvent>
               <q:dmEvent>
                  <q:dmEventTime>2020-07-17T10:20:13.463+02:00</q:dmEventTime>
                  <q:dmEventDescr>EV5: Datová zpráva byla dodána do datové schránky
příjemce. Je-li příjemcem datové zprávy orgán veřejné moci vystupující v postavení
orgánu veřejné moci, byla datová zpráva tímto okamžikem doručena.</q:dmEventDescr>
               </q:dmEvent>
               <q:dmEvent>
                  <q:dmEventTime>2020-07-27T10:20:13.000+02:00</q:dmEventTime>
                  <q:dmEventDescr>EV2: Uplynulo 10 dnů od dodání datové zprávy do
datové schránky příjemce, aniž by se do schránky přihlásila osoba, která má s ohledem
na rozsah svého oprávnění přístup k dodanému dokumentu (dle § 17, odst. 4, zákona č.
300/2008 Sb., v platném znění). Zpráva byla označena jako doručená fikcí. Byl-li
příjemcem datové zprávy orgán veřejné moci nevystupující v postavení orgánu veřejné
moci, byla datová zpráva doručena tímto okamžikem.</q:dmEventDescr>
               </q:dmEvent>
               <q:dmEvent>
                  <q:dmEventTime>2020-07-27T10:20:13.000+02:00</q:dmEventTime>
                  <q:dmEventDescr> EV6: V datové schránce adresáta nebyla v době od
okamžiku dodání zprávy do okamžiku doručení zprávy fikcí zavedena žádná osoba s
oprávněním přistupovat do datové schránky.</q:dmEventDescr>
               </q:dmEvent>
            </q:dmEvents>
         </q:dmDelivery>
         <q:dmStatus>
            <q:dmStatusCode>0000</q:dmStatusCode>
            <q:dmStatusMessage>Provedeno úspěšně.</q:dmStatusMessage>
         </q:dmStatus>
      </q:GetDeliveryInfoResponse>
```

Přibude další element `dmEvent` pro událost E6.

Tato úprava nevyžaduje změnu WSDL a XSD definic. Nicméně vývojáři musejí být informováni, protože mohou události v datech z WS nějakým způsobem zpracovávat a nová událost může způsobit „zmatek“. Pokud události jenom zobrazují, úprava není potřeba.

3.2.2 Mění se formát stažené zprávy?

Ne, formát zprávy se nemění, mění se pouze výčet událostí v doručence. Ze stažené zprávy (0do formátu podepsaného XML, resp. XML) se tento stav doručení fikcí nepozná. Nemění se formát webových služeb.

3.2.3 Koho se změna týká?

Aplikací nad schránkami OVM. Při dodávání zpráv do datových schránek PO může nastat legální situace, že ve zpřístupněné schránce není ani jeden uživatel.

Naopak netýká se aplikací nad schránkami neOVM – zprávy zasílané do OVM schránek se výkladem doručují již dodáním, schránka OVM musí zajistit, aby po celou dobu existence byla přítomná osoba s právem číst zprávy. Doručení fikcí nenastává u Poštovních zpráv – není třeba proto analyzovat Poštovní zprávy.

3.2.4 Co má aplikace s takovou doručenkou dělat?

Podle zákona je zpráva doručená bez ohledu na situaci s uživateli schránky. Nicméně příjemce zprávy doručené fikcí se může proti fikci soudně bránit a nelze vyloučit, že by uspěl s argumentem, že

skutečně neměl možnost se s obsahem zprávy seznámit. Ponecháváme na posouzení odesílatele, zda v tomto případě přistoupí k dalšímu pokusu o doručení alternativní cestou, tedy např. listinnou zásilkou.

3.2.5 Jak lze testovat?

V prostředí veřejného testu ISDS existuje zpřístupněná schránka typu PO bez uživatelů:

ID DS: **74yhsnc**
Název: **Firemní schránka bez uživatelů**
ICO: **43423647**

Pokud do této schránky bude zaslána datová zpráva, bude za 10 dní doručena fikcí a ve stažené doručence bude nová událost E6.