Nápověda k doložení bezpečnostních podmínek,

uvedených v části 1.6. Podmínek využívání přístupového rozhraní ISDS poskytovateli internetových služeb pod písmeny b), c), d), e) a f)

Obecně:

Smyslem níže uvedených podmínek je prokázat, že informační systém poskytovatele je zabezpečen alespoň na takové úrovni, jako je Informační systém datových schránek (viz např. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, Provozní řád ISDS atd.).

Způsob prokázání podmínky je vždy uvedením konkrétního a jednoznačného popisu splnění dané podmínky, ze kterého musí být správní orgán schopen jednoznačně posoudit, zda byla daná podmínka splněna, či nikoliv. Pokud vydal poskytovatel pro danou oblast interní směrnici, je možné dále přiložit (kromě konkrétního popisu způsobu splnění podmínky) její text nebo výtah, případně popis interních řídících aktů, norem a standardů.

Pokud poskytovatel provozuje více systémů, či používá různé způsoby zabezpečení, je třeba doložit výše uvedeným způsobem splnění pro každý z nich a to přehledným způsobem, aby správní orgán byl s to žádost posoudit.

Ke konkrétním podmínkám:

	Podmínka	Způsob prokázání
b)	Poskytovatel zajišťuje bezpečné vydávání a doručování přihlašovacích údajů k uživatelským účtům uživatelům, které zajišťuje jejich doručení při bezpečném ověření totožnosti.	Uvedení popisu způsobu a postupů, které jsou k uvedenému účelu použity.

Nápověda:

Smyslem této podmínky je prokázat, že bezpečnost vydávání přístupových údajů je minimálně na stejné úrovni, jako u Informačního systému datových schránek. Je tedy třeba, aby poskytovatel popsal, jakým způsobem je tak činěno v případě jím provozované aplikace. Pro posouzení splnění podmínky je potřeba znát alespoň následující údaje:

- jaké přihlašovací údaje pro přihlášení k uživatelským účtům poskytovatel používá (jméno, hesla, vícefaktorová autentizace, tokeny, čipové karty apod.),
- komu je vydává (vztah vlastníka účtu a jím pověřené osoby, zda mají každá svůj uživatelský účet atd.),
- jakým způsobem je vydává či doručuje vlastníkům uživatelským účtů (poštou do vlastních rukou, kurýrem či jinak),
- jakým způsobem je přitom ověřována jejich totožnost,
- jak je zajištěno, aby se s přihlašovacími údaji nemohl seznámit někdo jiný, včetně pracovníků poskytovatele.

c)	Poskytovatel zajišťuje obnovování a opakované vydávání přihlašovacích údajů k uživatelským účtům uživatelům, které zajišťuje jejich doručení při bezpečném ověření totožnosti.	Uvedení popisu způsobu a postupů, které jsou k uvedenému účelu použity.

Nápověda:
Smyslem této podmínky je prokázat, že poskytovatel zajišťuje obnovování a opakované vydávání přihlašovacích údajů k uživatelským účtům alespoň takovým způsobem, jako je tomu u ISDS. Pro posouzení této podmínky je potřeba znát alespoň následující údaje:

- jaké přihlašovací údaje pro přihlášení k uživatelským účtům poskytovatel používá (viz výše),
- jak je nastavena platnost těchto přihlašovacích údajů,
- při jakých příležitostech nastává obnovování či opakované vydávání přihlašovacích údajů (expirace, nahlášená ztráta, zneužití, preventivní krok ze strany poskytovatele apod.),
- jakým způsobem je opětovné vydávání zajištěno (popis procesu a možností) a jak je přitom ověřována totožnost vlastníků přihlašovacích údajů.

d)	Poskytovatel zajišťuje znepřístupnění uživatelských účtů a následné rušení příslušných přihlašovacích údajů, pokud nastanou skutečnosti, které uvedl v podmínkách poskytování služeb Poskytovatele a které znamenají porušení bezpečnosti ze strany uživatele.	Uvedení popisu způsobu a postupů, které jsou k uvedenému účelu použity.

Nápověda:
Smyslem této podmínky je doložit, že poskytovatel má řádně nastaven proces znepřístupnění uživatelských účtů a rušení přihlašovacích údajů například v situacích ztráty, odcizení přihlašovacích údajů, ukončení vztahu s klientem, úmrtí apod. Bude zkoumáno, zda tento proces odpovídá minimálně stejnému standardu, jako je nastaven u Informačního systému datových schránek. Pro posouzení žádosti je potřeba znát:

- jaké přihlašovací údaje jsou ze strany poskytovatele využívány (viz výše),
- v jakých situacích (při jakých skutečnostech) dochází k jejich zrušení a znepřístupnění uživatelských účtů,
- jakým způsobem je toto prováděno (popis procesu),
- jak má poskytovatel toto upraveno ve vlastních podmínkách poskytování služeb, včetně vymezení odpovědnosti uživatele a poskytovatele.

e)	Poskytovatel zajišťuje bezpečnost přihlašovacích údajů, které znemožňuje jejich zneužití	Uvedení popisu způsobu a postupů, které jsou k uvedenému účelu použity.

Nápověda:
Smyslem této podmínky je prokázat, že v informačním systému poskytovatele je zajištěna bezpečnost přihlašovacích údajů minimálně stejným způsobem, jako v případě Informačního systému datových schránek. K posouzení splnění této podmínky je třeba znát alespoň tyto údaje:

- jaké přihlašovací údaje či prostředky jsou ze strany poskytovatele využívány, (například zda je využíváno jméno a heslo, vícefaktorová autentizace, tedy např.

jednorázový bezpečnostní kód, certifikáty na tokenu nebo čipové kartě atd.),

- popis jejich technických parametrů (požadavky na tvorbu jmen a hesel, technické standardy využívaných technických prostředků, jaké certifikáty jsou využívány a kdo je vydává, pokud je využíván jednorázový bezpečnostní kód, jakým způsobem a jak je generován apod.),
- popis způsobu vkládání přihlašovacích jmen a jejich přenosu (například jak vypadá přístupová stránka aplikace uživatele, způsob ochrany proti keyloggerům - virtuální klávesnice - ochrana proti opakovanému zadání nesprávné kombinace jména a hesla, způsob šifrování komunikace - https - ochrana proti phishingu apod.)

f)	Poskytovatel zajišťuje, že hesla a další neveřejné údaje, které se využívají pro přihlašování k uživatelským účtům, nejsou uloženy v otevřené podobě, ale jsou adekvátně fyzicky a logicky (kryptograficky) chráněny, aby bylo znemožněno jejich zneužití neoprávněnými osobami.	Uvedení popisu způsobu a postupů, které jsou k uvedenému účelu použity.

Nápověda:

Smyslem této podmínky je popsat a doložit, že hesla a další neveřejné údaje jsou v interních systémech poskytovatele uloženy a zabezpečeny takovým způsobem, který znemožňuje jejich zneužití zejména ze strany interních pracovníků, ale i případných útočníků. Poskytovatel by měl popsat:

- o jaké údaje se jedná (jméno, heslo, různé další údaje pro ověření identity),
- jakým způsobem jsou uloženy v jeho interních systémech a jak jsou fyzicky a logicky (kryptograficky) chráněny,
- jak je zajištěno, aby se s nimi nemohl seznámit žádný interní pracovník,
- jak je zajištěno, aby se k nim nemohl dostat nikdo útokem zvenčí,
- jaké kontrolní mechanismy jsou používány pro ověření funkčnosti výše uvedených opatření.