1 Užitné vlastnosti

- HW zařízením, tedy „nosičem“ druhého autentizačního faktoru bude mobilní telefon, příp. tablet. Předpokládáme omezení na kategorii „smartphone“. Pokud bude zvoleno řešení založené na mobilní aplikaci, není nutné omezovat použití na mobilní telefony, lze pak připustit i jiná mobilní zařízení, např. tablety. Případná mobilní aplikace musí být dostupná nejméně na platformě iOS a Android.
- MEP umožní přihlášení v prostředí jiných mobilních aplikací instalovaných na stejném zařízení i přihlášení do webových aplikací na tomto i jiném zařízení, jako je např. počítač.
- Používání MEP musí být maximálně jednoduché. Všechny obslužné procesy by měly probíhat automatizovaně či v pozadí a nevyžadovat administrativní činnosti od uživatelů. Přihlašovací údaje by neměly být založeny na jménu / heslu / OTP, ale na jiném inovativním řešení, které bude dostatečně bezpečné, ale přitom uživatelsky snadno použitelné.
- MEP umožní uživateli jeho přenos z jednoho mobilního zařízení na druhý bez nutnosti návštěvy kontaktního místa veřejné správy.
- MEP umožní uživateli použít další mobilní zařízení jako alternativní prostředek s rovnocennou funkčností.
- MEP bude navržen tak, aby mohl splňovat nejméně značnou úroveň záruky ve smyslu Nařízení eIDAS a prováděcích předpisů.
- Zablokování prostředku bude uživateli umožněno učinit na kontaktních místech veřejné správy (fáze 2) anebo vzdáleně, bez nutnosti návštěvy kontaktního místa veřejné správy, za použití druhého prostředku.

2 Bezpečnostní vlastnosti

2.1 Ochrana soukromí

- MEP musí mít vestavěnu ochranu soukromí při autentizaci, ochranu osobních informací během autentizace a ochranu proti neoprávněnému propojování osobních údajů mezi spoléhajícími stranami.

2.2 Řízené používání druhého faktoru

- Prostředky, které umožní řídit používání druhého faktoru, otevírají systémové možnosti řešení problému rizika kompromitace druhého faktoru. Zároveň přinášejí možnosti vyšší bezpečnosti, vyšší efektivity a lepšího uživatelského vnímání především v situacích, kdy používání druhého faktoru není nutné.
- Přihlašování pomocí MEP bude dvoufaktorové, a to na základě kombinace minimálně dvou různých z následujících tří typů faktorů. Něco, co mám – předmět, např. smartphone, něco co znám – heslo nebo PIN a něco, co jsem – biometrika. Kromě zadání faktoru typu „něco co znám“, nebude uživatel ručně zadávat žádné přihlašovací údaje.
- V případech, kdy to dovolí klientská aplikace, prostředek umožní, aby externí aplikace určila, zda postačí přihlášení pomocí jediného faktoru.

2.3 Automatická správa kryptografických klíčů

- MEP musí zajistit obnovu kryptografických klíčů bez potřeby součinnosti uživatele. Uživatel nemusí provádět žádné úkony k zajištění obnovy kryptografických klíčů, o obnovu kryptografických klíčů se nemusí nijak starat. Infrastruktura MEP zajistí obnovu kryptografických klíčů automaticky sama.

2.4 Samoobslužné zotavení z individuálních mimořádných situací

- MEP budou podporovat řešení individuálních mimořádných situací samoobsluhou, a to zejména v běžných individuálních mimořádných situacích jako je technická porucha eID prostředku, ztráta, krádež, výměna zařízení za nové (např. modernější chytrý telefon). Samoobslužné řešení mimořádných situací nesníží bezpečnost eID prostředků.

2.5 Automatizované zotavení z hromadných krizových situací

- MEP musí předem počítat s tím, že může nastat krizová situace, která zasáhne všechny prostředky najednou. MEP musí mít vestavěny automatizované postupy zotavení z krizových situací, které bude možné provádět hromadně za běhu, a to bez nutnosti znovu aktivovat prostředek na registračním pracovišti nebo bez nutnosti upgrade firmware vyžadujícího návštěvu takového pracoviště.