

Souhrnný protokol o testování ZFO

Software602 Form Filler: integrita, chybná data a duplicity

Verze 2.1, stav k 24. 9. 2026. Technické testy byly zaznamenány 23. 9. 2026; doplňující uživatelské pozorování při tisku bylo dodáno 24. 9. 2026. Dokument slouží jako věcný podklad pro veřejnou diskusi. Není adresován konkrétní instituci.

Hlavní zjištění

Software602 Form Filler 4.81.6.0 u konkrétní pozměněné doručky oznámil neporušený obsah a v laboratorním prostředí po kontrole odvolání také platnou pečeť a důvěryhodný neodvolaný certifikát. Samostatná kontrola OpenSSL a Datovka CZ.NIC přitom pro stejný vzorek odhalily nesoulad podpisu s obsahem. Jde o doložené chybné kladné hlášení v popsané konfiguraci, jehož vnitřní příčina nebyla určena.

Další syntetické testy ukázaly, že Software602 Form Filler zobrazil neexistující datum 92.13.1200 a u dvou rozdílných podepsaných předmětů vybral první v pořadí XML. Tyto dvě vlastnosti samy nepředstavují porušení kryptografického podpisu: chybné či duplicitní údaje byly do dokumentů vloženy už před podpisem.

Uživatel dále doložil, že po vyvolání tisku přibude hlášení „Byly provedeny změny“, zatímco „Obsah je neporušen“ zůstává v panelu i podrobném dialogu. Doplněná kontrola ukázala stejné hlášení i u neporušeného originálu a nového syntetického vzorku; soubory zůstaly beze změny a jejich podpisy prošly OpenSSL. Samotné hlášení tedy nerozlišuje porušení integrity.

Co prokázáno nebylo

Nebyla prokázána možnost zobrazit alternativní nepodepsanou hodnotu jako podepsanou. Nebylo prokázáno prolomení pečeti, získání soukromého klíče, napadení aplikace ani chyba serveru ISDS. Nebyl testován serverový způsob načítání dat, a proto se nevyjadřujeme ani k jeho nenapadnutelnosti. Nelze automaticky zobecňovat na jiné verze či všechny instalace.

Charakter a veřejný rozsah

Retrospektivní technický záznam sestavený s pomocí asistenta Codex z uchovaných souborů, výsledků kontrol a snímků aplikací. Nejde o znalecký posudek ani úplnou validaci dle ETSI/eIDAS. Veřejná příloha obsahuje pouze fiktivní syntetické vzorky a vybrané snímky bez údajů účastníků skutečných zpráv. Skutečné doručky a jejich pozměněná kopie nejsou ve veřejném balíčku obsaženy.

1. Vzorky, prostředí a význam pečeti

Označení skutečných vstupů a odvozené kopie

Originál číslo 1 (neporušený): dodaná doručenka z roku 2022. Originál číslo 2 (neporušený): odpovídající datová zpráva s jednou PDF přílohou. Originál číslo 3 (neporušený): novější dodaná doručenka z roku 2026. Falsum číslo 1 (zásah do dat): oddělená, výslovně označená laboratorní kopie odvozená ze vzorku Originál číslo 3 (neporušený).

Výraz „neporušený“ označuje zachování dodaných bajtů a úspěšnou kontrolu jejich kryptografické integrity. Není samostatným potvrzením pravdivosti všech údajů ani úplné historické důvěryhodnosti. Vstupy poskytl uživatel; nebyly nezávisle znovu získány z ISDS. Přesná identifikace pomocí SHA-256 je v katalogu příloh.

Syntetické vzorky

Dvě dvojice pro kontrolu integrity (RSA PKCS#1/SHA-256 a RSA-PSS/SHA-512), tři vzorky pro neplatné datum a čtyři pro duplicitu předmětu. Původní sada má 11 veřejných ZFO; doplňující kontrola tisku přidává dvanáctý vzorek. Mají fiktivní odesílatele a příjemce, ID zprávy 0 a označení, že nejde o doklad ISDS. Byly podepsány jednorázovými testovacími klíči; soukromé klíče nebyly uloženy. Samostatná kontrolní serializace novějšího originálu je zachována pouze v neveřejné pracovní evidenci.

Prostředí

Software602 Form Filler 4.81.6.0 na Windows Home/Core, build 26200. OpenSSL 3.0.13 pro samostatné ověření CMS; další analýza prostřednictvím knihoven ASN.1 a cryptography. Datovka CZ.NIC 4.29.5 x64, Qt 6.10.3, libdatovka 0.7.4, OpenSSL 3.6.3, přenosný čistý profil bez účtu datové schránky. Použito místní otevření ZFO, nikoli ověření souboru serverem ISDS.

Část testů Software602 Form Filler proběhla v Sandboxie Plus 1.18.4. Jde o izolaci zápisů a registru, nikoli samostatný virtuální počítač. Syntetickému certifikátu byla pro jednu etapu nastavena důvěra pouze v laboratorním úložišti; kontrola před a po jej nenašla v kořenových úložištích hostitele. Testy neplatného data a duplicit proběhly mimo Sandboxie. U dodatečných uživatelských snímků není verze ani prostředí samostatně doloženo.

Co chrání podpis

Zkoumané ZFO jsou kontejnery CMS SignedData s vloženým XML. Podpis chrání kontrolní otisk přesných bajtů celého vloženého XML, včetně předmětu, EV0, časů a případných příloh. Nechrání automaticky každý bajt obalu souboru. Ve zkoumaných doručenkách nebyl nalezen alternativní nepodepsaný zdroj EV0. Platný podpis dokládá integritu dat; sám nezaručuje platné kalendářní datum, správnost schématu ani jednoznačnost duplicit.

2. Rozbor originálů a hlavní test integrity

Původní rozbor

Originál číslo 1 (neporušený) a Originál číslo 2 (neporušený) mají vnější podpis RSA PKCS#1 v1.5 se SHA-256. XML má 9 653, respektive 250 039 bajtů. Vnější podpisy a jejich vazby na obsah prošly matematickou kontrolou i OpenSSL. V doručence není vnější razítko podpisu; zpráva je obsahuje. Podací razítko je odlišná vrstva a jeho otisk odpovídá dmHash. Transformace pro nezávislé přepočtení dmHash z podávané zprávy nebyla potvrzena.

Vložená PDF příloha má 180 749 bajtů a jednu stránku; obsahuje samostatný matematicky ověřený podpis a vlastní časové razítko. Historické odvolání a úplná dlouhodobá důvěryhodnost všech certifikátů nebyly ověřeny. První pokus o GUI kontrolu těchto dvou originálů nebyl technicky úspěšný, proto pro ně neuvádíme potvrzený výsledek zobrazení.

Originál číslo 3 (neporušený) má XML o 9 668 bajtech, bez příloh; používá RSA-PSS se SHA-512, MGF1 SHA-512 a solí 64 bajtů. Podpis odpovídá obsahu. Kontrola řetězců Windows pro certifikát pečeti a podacího razítka vrátila úspěch; surové revokační odpovědi ani úplná validace evropských seznamů důvěryhodných služeb nebyly archivovány. Datovka CZ.NIC potvrdila platný podpis i certifikát při otevření přesné cesty. U raného kladného zobrazení v Software602 Form Filler byla výhrada k úplné identifikaci cesty okna.

Falsum číslo 1 (zásah do dat)

Ve zvláštní kopii byl předmět změněn na výrazné označení laboratorního testu FALSUM a EV0 posunuto o jeden den do budoucnosti. Ostatní textové hodnoty byly zachovány. Původní podpis, podepsané atributy a vložené certifikáty zůstaly stejné; nevznikla nová pečť. Samotná kontrolní serializace beze změny XML prošla OpenSSL, pozměněná kopie selhala na content verify error.

Software602 Form Filler v laboratorním boxu zobrazil změněná data a po kontrole odvolání hlásil:

„Doručenka byla opatřena platnou elektronickou značkou/pečetí. Obsah je neporušen.“ Certifikát označil za důvěryhodný a neodvolaný. Datovka CZ.NIC naproti tomu uvedla: „Neplatný -- Podpis zprávy a její obsah si neodpovídají!“

Závěr a jeho hranice

Byl doložen rozpor mezi kladným hlášením Software602 Form Filler a nezávislou kontrolou obsahu. Příčina může ležet v ověřování, předání jeho výsledku nebo jeho zobrazení; nebyla rozlišena. Platné podací razítko či důvěryhodný certifikát tento nesoulad nenapravují. Opakování tohoto konkrétního testu na čisté nezávislé instalaci mimo Sandboxie dosud nebylo doloženo. Veřejný čtenář nemůže tento reálný vzorek přepočítat z veřejné přílohy, protože obsahuje neveřejné údaje.

3. Syntetické kontroly a neplatná data

Dvojice s porušením integrity

U obou syntetických dvojic byla varianta A podepsána s EV0 1. 1. 2000, 10:00:00. U varianty B se den po podpisu změnil na 2. 1. 2000. OpenSSL přijímá A a odmítá B. Software602 Form Filler u obou variant obou dvojic hlásil neporušený obsah; certifikáty byly mimo laboratorní úložiště nedůvěryhodné. Raná dvojice má záznam přímého pozorování zabezpečení, ale samostatný archivovaný snímek tohoto dialogu se nezachoval.

U dvojice RSA-PSS/SHA-512 bylo navíc provedeno ověření s výslovně určeným testovacím certifikátem jako důvěryhodným v samostatné kontrole OpenSSL: A prošlo, B opět selhalo. Důvěra v certifikát tak nezměnila výsledek kontroly integrity.

Po laboratorním nastavení důvěry Software602 Form Filler označil certifikát obou variant za důvěryhodný, s dosud neověřeným odvoláním, a nadále hlásil neporušený obsah. Nejde o úplné ověření pečeti ISDS. Datovka CZ.NIC u pozměněné varianty RSA-PSS/SHA-512 výslovně odmítla nesoulad podpisu a obsahu; ostatní syntetické varianty v této etapě nebyly Datovkou testovány.

Neplatné datum vložené před podpisem

Následující tři nové vzorky byly podepsány až po nastavení údaje EV0. Všechny mají matematicky správný podpis. Proto jde o zpracování neplatných dat, nikoli o selhání integrity.

Kontrola: 2000-01-01T10:00:00+01:00 → 01.01.2000 v 10:00:00.

Neexistující den a měsíc: 1200-13-92T10:00:00+01:00 → 92.13.1200 v 10:00:00.

Doslovný text: 92.13.1200 → 00..1.92.1 v.

Software602 Form Filler všechny tři vzorky otevřel. Na zachycených obrazovkách nebylo upozornění na neplatné datum. Panel hlásil neporušený obsah a upozornění na stav některého z certifikátů. Podrobný stav důvěry a odvolání nebyl v této etapě doložen.

Interpretace

Pozorování je slučitelné s formátováním částí řetězce bez účinné kalendářní kontroly v této cestě zobrazení; přesná implementace nebyla zjištěna. Hlášení neporušenosti je u těchto tří vzorků v souladu s OpenSSL. Ze správného podpisu nelze odvozovat správnost data. Chování ISDS při přijetí takových hodnot se netestovalo.

4. Duplicity: provedené a neprovedené testy

Provedeno: dva předměty uvnitř podepsaného XML

Čtyři syntetické vzorky obsahují jednu nebo dvě hodnoty dmAnnotation pod stejným rodičem dmDm a ve stejném jmenném prostoru. Duplicity jsou sousední prvky; nejde o běžný seznam událostí. Všechny hodnoty byly vloženy před podpisem a celé XML následně podepsáno novým testovacím certifikátem. V žádném ze vzorků nejsou nepodepsané atributy CMS.

Pouze ALFA → Software602 Form Filler zobrazil ALFA.

Pouze BETA → Software602 Form Filler zobrazil BETA.

ALFA, potom BETA → Software602 Form Filler zobrazil ALFA.

BETA, potom ALFA → Software602 Form Filler zobrazil BETA.

Všechny podpisy prošly OpenSSL a všechny soubory byly otevřeny. V zachyceném formuláři nebylo upozornění na duplicitu. Pro tuto konkrétní strukturu tedy rozhodovalo první pořadí předmětu. Druhá hodnota nebyla zobrazena jako další předmět. Není tím doloženo, že interně nebyla vůbec zpracována.

Obě hodnoty chrání podpis. Výsledek není důkazem obejití pečeti, čtení z nepodepsaných dat ani automaticky obecnou bezpečnostní chybou. Ukazuje nejednoznačnost, kterou uživatel z tohoto zobrazení nepozná. Soulad kompletních syntetických dokumentů s produkčním XSD nebyl potvrzen. Chování dalších polí nelze odvodit jen z předmětu.

Neprovedeno: podepsaná a nepodepsaná alternativa

V diskusi byl navržen pokus s rozdílnými hodnotami stejného údaje v podepsané a nepodepsané části. Varianty se týkaly EV0, neplatného data, předmětu i obecného údaje. Byla vyslovena nabídka laboratorního provedení, která byla následně omezena; soubor pro tento pokus nevznikl a test neproběhl.

Asistent tuto konstrukci odmítl s ohledem na původní kontext požadavku na nepozorovatelné pozměnění doručky. Odmítnutí je omezením provedené práce, nikoli důkazem nemožnosti či existence chyby. Nereálné datum nebo nahrazení času předmětem na stavu NEPROVEDENO nic nemění. Následující test dvou podepsaných hodnot tento odmítnutý pokus nenahradil.

Dále neprovedeno

Nebylo provedeno sledování zdroje zobrazovaného XML uzlu uvnitř procesu, rozbor zdrojového kódu ani porovnání interních dat předaných ověřování a vykreslení. Neproběhl samostatný test duplicitního EV0 uvnitř podepsaného XML, jiných umístění, jmenných prostorů ani shodných duplicit. O těchto případech nejsou výsledky.

Souborová kontrola skutečných doruček a jedné syntetické kopie našla vždy jedinou událost EV0 a jediný výskyt jejího přesného časového řetězce. Nebyly nalezeny nepodepsané atributy CMS ani připojená data za kontejnerem. Tato kontrola omezené sady souborů nenahrazuje rozbor všech možných vstupů aplikace.

5. Kontrola tisku: doplněný srovnávací pokus

Dřívější pozorování a nová kontrola

Uživatelské snímky pozměněné doručanky zachycovaly hlášení „Byly provedeny změny“ po vyvolání tisku současně s tvrzením „Obsah je neporušen“. Dne 24. 9. 2026 byla kontrola doplněna o neporušený originál a nový syntetický vzorek.

Originál číslo 3 (neporušený)

Byla otevřena přesně identifikovaná bitově shodná kopie originálu v Software602 Form Filler 4.81.6.0 mimo Sandboxie. Před tiskem se zobrazovalo „Obsah je neporušen“ bez červeného hlášení. Po kliknutí na Vytisknout se objevil tiskový dialog, červené „Byly provedeny změny“ a hvězdička u záložky Doručenka. Po zrušení dialogu klávesou Escape zůstala obě hlášení. Nebyl zadán tisk ani uložení změn.

SHA-256 byl před a po shodný s katalogem originálu. Následné OpenSSL cms -verify -noverify vrátilo CMS Verification successful. Jde o ověření shody podpisu s obsahem, nikoli nové úplné ověření důvěry certifikátu. Soubor na disku se nezměnil. Soukromé snímky jsou uchovány odděleně.

Nový veřejný kontrolní vzorek

TEST-TISK-A.zfo obsahuje výlučně fiktivní údaje a předmět KONTROLA TISKU - SYNTETICKÝ VZOREK - NENI DOKLAD ISDS. Byl nově podepsán testovacím certifikátem PRINT CONTROL LAB - NOT ISDS; klíč nebyl uložen a certifikát nebyl přidán mezi důvěryhodné. Soubor nebyl po podpisu upravován. Kontrola OpenSSL před a po byla úspěšná a SHA-256 zůstal shodný.

Před tiskem aplikace hlásila neporušený obsah a upozornění na stav certifikátu. Po vyvolání tisku přibýlo červené hlášení změn. Následný snímek ukazuje uzavřený tiskový dialog a podrobnosti zabezpečení: obsah neporušen, testovací certifikát nedůvěryhodný. V tomto mezikroku nástroj zaznamenal zásah uživatele, proto přesný způsob uzavření dialogu a otevření podrobností není přisuzován automatizaci. Rozhodné objevení červeného hlášení už při vyvolání tisku bylo zachyceno před tímto zásahem.

Závěr a rozsah

Hlášení „Byly provedeny změny“ se objevuje také u neporušeného originálu i neporušeného syntetického vzorku. Samotý nerozlišuje zásah do podepsaných dat. Pozorování je slučitelné se změnou pracovního formuláře při přípravě tisku; přesná vnitřní příčina není určena. Nejde o důkaz, že aplikace při tisku dodatečně odhalí porušení pečeti.

Pozměněná kopie nebyla v tomto doplňujícím pokusu znovu otevřena; srovnání s ní vychází z dřívějších uživatelských snímků. Hlavní nález chybného kladného hlášení integrity tím není vyvrácen. Opakování hlavního nálezu na čisté instalaci a porovnání dalších verzí zůstávají neprovedeny.

6. Omezení a evidence veřejné verze

Stav důkazů

Přímo doložené jsou kontrolní součty a výsledky OpenSSL, uchované vzorky a snímky zobrazení. Pro testy neplatných dat a duplicit jsou ve veřejné příloze všechny použité ZFO, úplná XML a snímky. Veřejná příloha obsahuje také obě starší syntetické dvojice a vybrané snímky jejich zobrazení a hlášení integrity.

Původní pozorování tisku pozměněné kopie je uživatelský příspěvek; doplňující kontrola neporušeného originálu byla provedena přímo a je popsána v kapitole 5. Jeho původní snímky i skutečné originály a Falsum číslo 1 (zásah do dat) zůstávají v neveřejné pracovní evidenci kvůli osobním údajům. Veřejný protokol uvádí jejich výsledky a identifikační otisky; neumožňuje sám nezávisle přezkoumat celý tento neveřejný materiál.

Názvosloví

Označení Originál číslo 1 (neporušený), Originál číslo 2 (neporušený), Originál číslo 3 (neporušený) a Falsum číslo 1 (zásah do dat) jsou popisné názvy vzorků v tomto dokumentu. Číslo falsum označuje samostatnou řadu a neznámá, že vychází z prvního originálu; vychází z třetího. Syntetické vzorky zůstávají odlišeny popisem testu a variantou.

Co veřejné podklady nezahrnují

Neobsahují skutečné zprávy, osobní identifikátory účastníků, původní PDF přílohu, soukromé klíče ani instalátory. Původní rozsáhlé předávací protokoly se zde nerepublikují; některé zachycovaly jen průběžné stavy a obsahovaly adresáty. Tento souhrn je samostatná veřejná verze a zachovává jejich důkazní omezení.

Úplnost ověření

Neproběhl úplný audit aplikace, úplná validace produkčních schémat, nezávislé serverové ověření zpráv ani úplná dlouhodobá validace všech certifikátů. Surové CRL/OCSP odpovědi nebyly archivovány. Kontrola OpenSSL s -noverify vynechává ověření certifikačního řetězce, nikoli matematickou kontrolu podpisu a obsahu. Nové sestavení tohoto dokumentu není novým opakováním GUI testů.

Původní skutečné soubory nebyly přepsány. Otisky označují zachované bajty, nikoli jejich historii před předáním. Pojem „kompromitace aplikace“ tento protokol nepoužívá jako závěr: není doloženo převzetí aplikace ani odcizení klíčů. Přesným zjištěním zůstává chybné kladné hlášení integrity u konkrétních vzorků a popsané chování při zpracování chybných a duplicitních dat.

Veřejný katalog

Katalog-vzorku.json uvádí názvy, velikosti, SHA-256 a dostupnost jednotlivých vzorků. Veřejné syntetické vzorky jsou v adresáři vzorky, snímky v adresáři snímky. Manifest souborů a SHA256SUMS.txt umožňují ověřit přiložený obsah. Tyto součty ani protokol nejsou elektronickým podpisem či časovým razítkem. Součástí je i samostatný text pro web a jeho statická HTML verze. Nic nebylo automaticky publikováno.

7. Identifikace neveřejných vzorků

Originál číslo 1 (neporušený)

12933 bajtů

SHA-256: 89c11ab78616ec28872ef168a0d0f5057d9d0ca7f6b0ec915b3edcfe2b5377f4

Originál číslo 2 (neporušený)

259317 bajtů

SHA-256: 477449ee507740400f512243121953ce8e7696ba3894dacfda50448254274238

Originál číslo 3 (neporušený)

13286 bajtů

SHA-256: d85c29aac73f4a31e1ebca1d4ae68d4c3c66ee8a8b4c62016ecb8663487f3206

Falsum číslo 1 (zásah do dat)

13283 bajtů

SHA-256: befcbef1dffb8a7084138cb227bfe57b1feae434cd0f1c8abf3d9a40f0c80d00

Kontrolní serializace bez změny XML

13246 bajtů

SHA-256: beaafc66d3c5f843460f5eb080cc6c6edbf25f8f48e72b0181e6ddab429fd12b

Přesné názvy skutečných zpráv a jejich identifikátory nejsou v této veřejné verzi uvedeny. Otisky slouží k jednoznačné návaznosti na uchovanou pracovní evidenci. Katalog veřejných syntetických vzorků s otisky je přiložen samostatně.

8. Snímky: neplatné datum

Podepsané neexistující datum je zobrazeno jako 92.13.1200 v 10:00:00.

Doslovný vstup 92.13.1200 je zobrazen jako 00..1.92.1 v.

9. Snímky: pořadí duplicitních předmětů

Pořadí ALFA–BETA: zobrazen první předmět ALFA.

TEST-DUP-AB.zfo - Software602 Form Filler

Odesílatel: TEST - FIKTIVNÍ ODESÍLATEL - TEST - NEEEXISTUJÍCÍ ADRESA

Doručenka [Vytisknout] [Uložit]

Předmět: TEST HODNOTA ALFA - NENI DOKLAD ISDS	Události zprávy: 01.01.2000 v 10:00:00 EV0: SYNTETICKÝ TEST - FIKTIVNÍ PODÁNÍ, NENI DOKLAD ISDS.	Adresát: TEST - FIKTIVNÍ PŘIJEMCE TEST - NEEEXISTUJÍCÍ ADRESA	Zmocnění: Nezadáno Odstavec: Nezadáno Naše čís. jednací: Nezadáno Naše spisová zn.: Nezadáno Vaše čís. jednací: Nezadáno Vaše spisová zn.: Nezadáno K rukám: Nezadáno Do vlastních rukou: Ne Zakázáno doručení fiktiv: Ne
ID zprávy: 0		ID schránky: bbbbbb	
Datum a čas dodání: 03.01.2000 v 12:00:00			
Datum a čas doručení: 03.01.2000 v 13:00:00			

[Zavřít]

Informace o formuláři

Zabezpečení

Doručenka byla opatřena elektronickou značkou/pečetí. Obsah je neporušen. Stav některého z certifikátů vyžaduje pozornost! [Klikněte pro více informací...](#)

Informace k poli

Pořadí BETA–ALFA: zobrazen první předmět BETA.

TEST-DUP-BA.zfo - Software602 Form Filler

Odesílatel: TEST - FIKTIVNÍ ODESÍLATEL - TEST - NEEEXISTUJÍCÍ ADRESA

Doručenka [Vytisknout] [Uložit]

Předmět: TEST HODNOTA BETA - NENI DOKLAD ISDS	Události zprávy: 01.01.2000 v 10:00:00 EV0: SYNTETICKÝ TEST - FIKTIVNÍ PODÁNÍ, NENI DOKLAD ISDS.	Adresát: TEST - FIKTIVNÍ PŘIJEMCE TEST - NEEEXISTUJÍCÍ ADRESA	Zmocnění: Nezadáno Odstavec: Nezadáno Naše čís. jednací: Nezadáno Naše spisová zn.: Nezadáno Vaše čís. jednací: Nezadáno Vaše spisová zn.: Nezadáno K rukám: Nezadáno Do vlastních rukou: Ne Zakázáno doručení fiktiv: Ne
ID zprávy: 0		ID schránky: bbbbbb	
Datum a čas dodání: 03.01.2000 v 12:00:00			
Datum a čas doručení: 03.01.2000 v 13:00:00			

[Zavřít]

Informace o formuláři

Zabezpečení

Doručenka byla opatřena elektronickou značkou/pečetí. Obsah je neporušen. Stav některého z certifikátů vyžaduje pozornost! [Klikněte pro více informací...](#)

Informace k poli