Paperless Signatur – Bezpieczeństwo

Wersja 1.1

Billennium

Spis treści

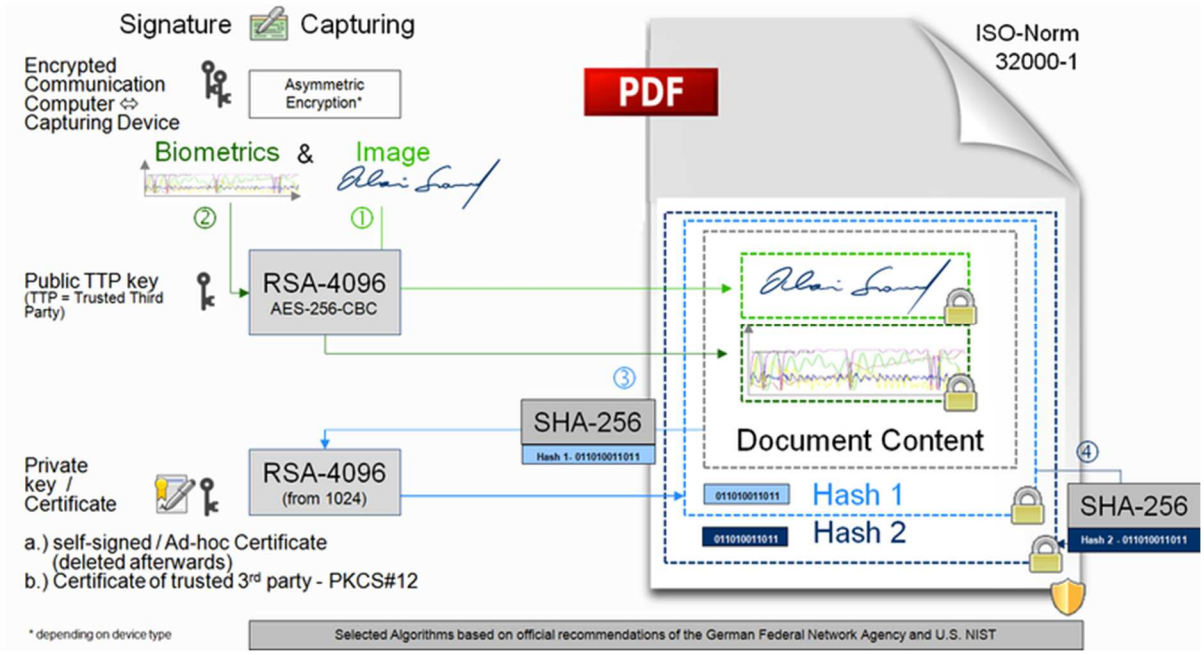
1 Historia wersji dokumentu

Wersja	Data	Autor	Zakres zmian
1.0	2016-01-25	Piotr Aftewicz	Utworzenie dokumentu.
1.1	2016-02-11	Piotr Aftewicz	Aktualizacja dokumentu.

2 Opis zabezpieczeń

Celem niniejszego dokumentu jest opisanie zabezpieczeń jakie są stosowane w ramach technologii Odręcznego Podpisu Elektronicznego w oparciu o narzędzia firmy Kofax.

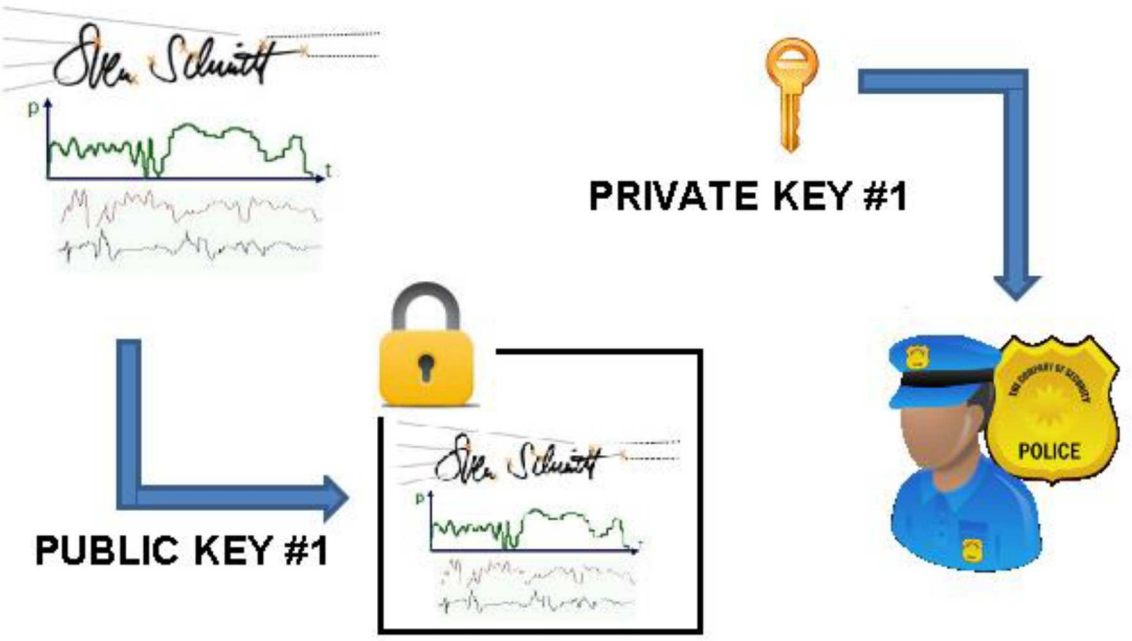
Całość zabezpieczenia dokumentu można zawrzeć w następujących 7 krokach, opisanych w poniższych rozdziałach.



2.1 Szyfrowane połączenie

Aplikacja nawiązuje szyfrowane połączenie z urządzeniem do podpisywania przy wykorzystaniu algorytmu AES-256. Para kluczy jest generowana dla każdej nowej sesji. Zastosowanie kluczy może być oparte o algorytm RSA lub Diffie-Hellman-Merkle.

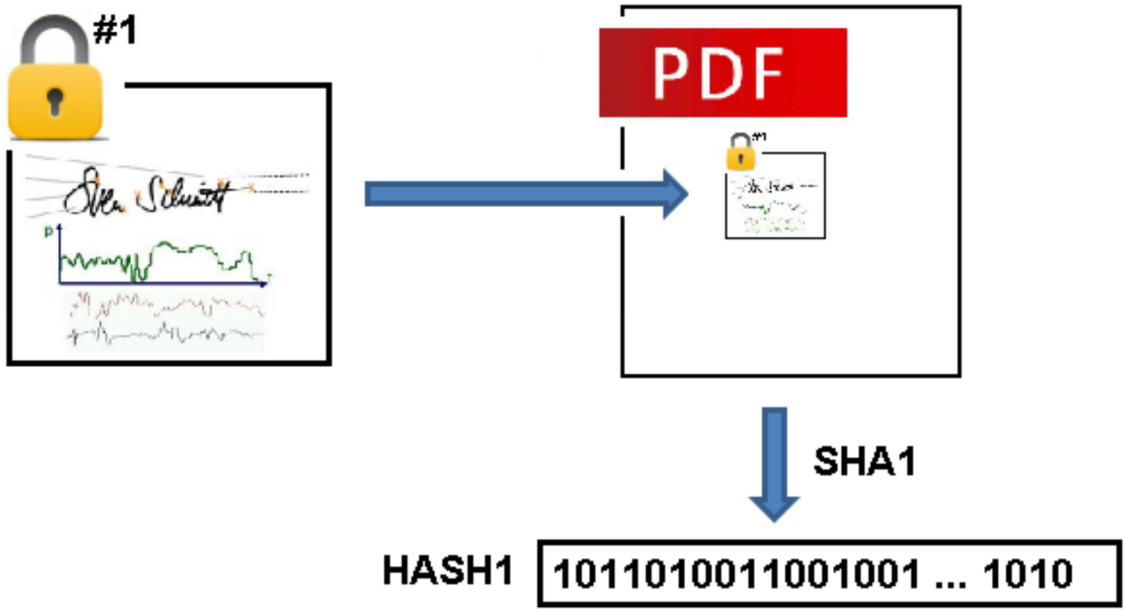
2.2 Podpisanie danych kluczem publicznym



Po wykonaniu podpisu na urządzeniu dane są podpisywane przy wykorzystaniu klucza publicznego. Klucz prywatny wykorzystany do podpisania danych biometrycznych powinien być składowany przez zewnętrzną zaufaną stronę trzecią. Lista instytucji tego typu w Polsce:

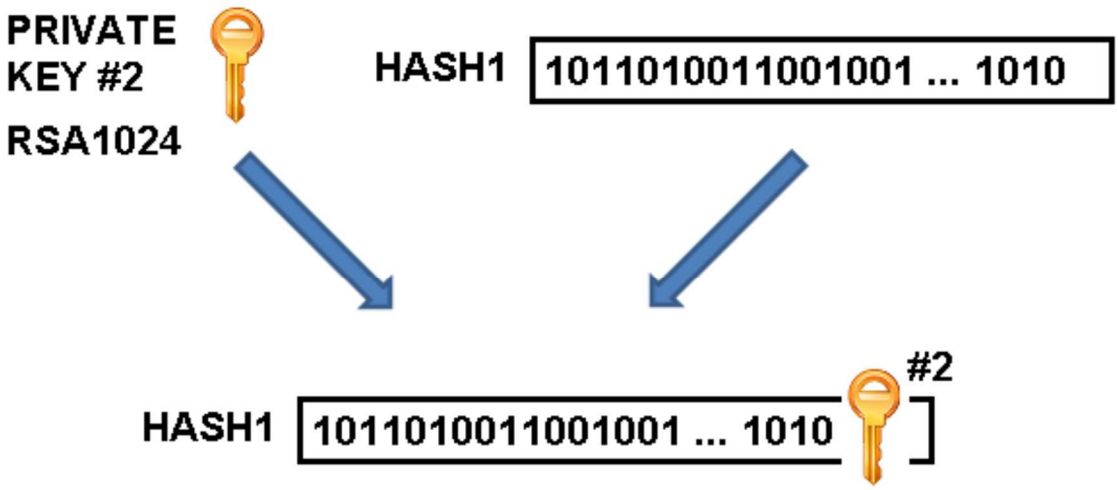
1. Krajowa Izba Rozliczeniowa SA (Szafir)
2. Polska Wytwórnia Papierów Wartościowych SA (Sigillum)
3. Unizeto Technologies SA (Certum)
4. Eurocert.pl
5. Enigma Systemy Ochrony Informacji Sp. z o.o. (CenCert).

2.3 Szyfrowanie danych



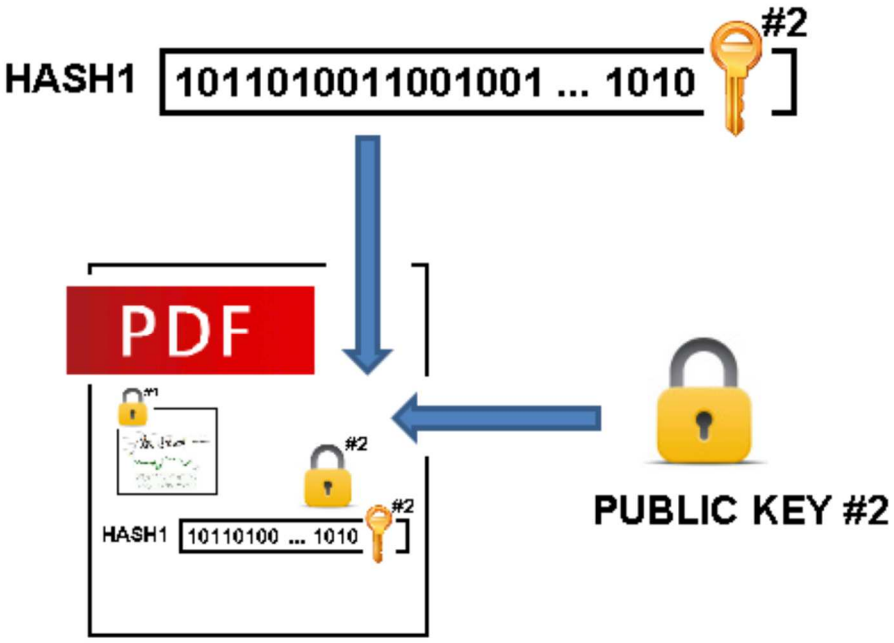
Zabezpieczone dane biometryczne są umieszczane w dokumencie a następnie dokument jest szyfrowany przy wykorzystaniu klucza SHA-2.

2.4 Podpisanie zaszyfrowanych danych



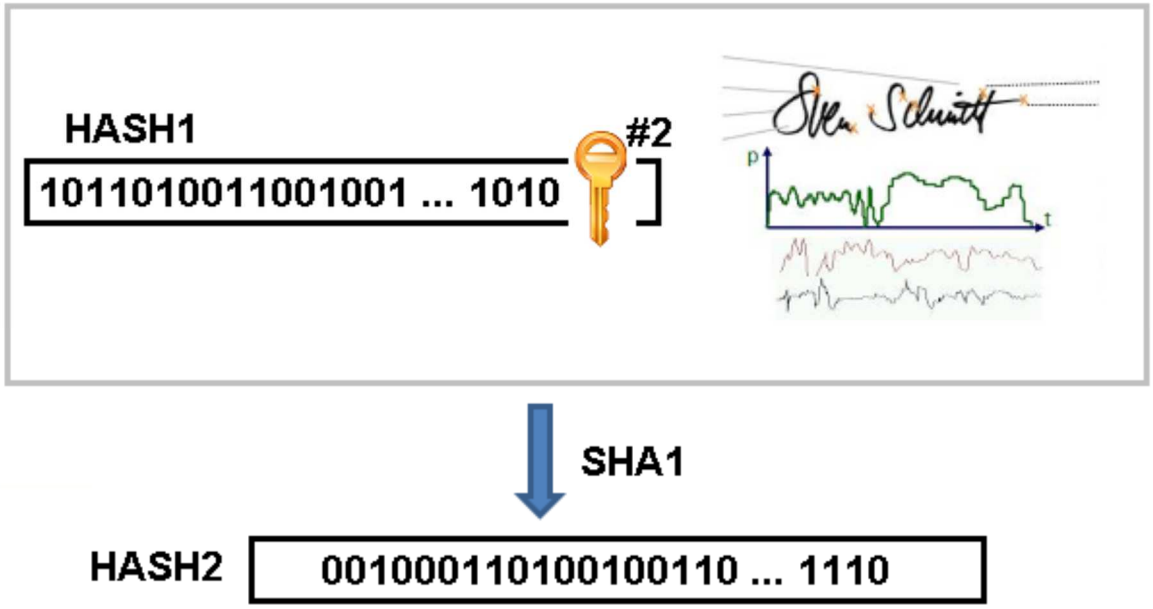
Hash wygenerowany w poprzednim kroku jest podpisywany za pomocą wygenerowanego klucza prywatnego (RSA-2048 lub RSA-4096). Alternatywą jest zastosowanie klucza prywatnego przechowywanego przez zaufaną stronę trzecią.

2.5 Umieszczenie danych w dokumencie



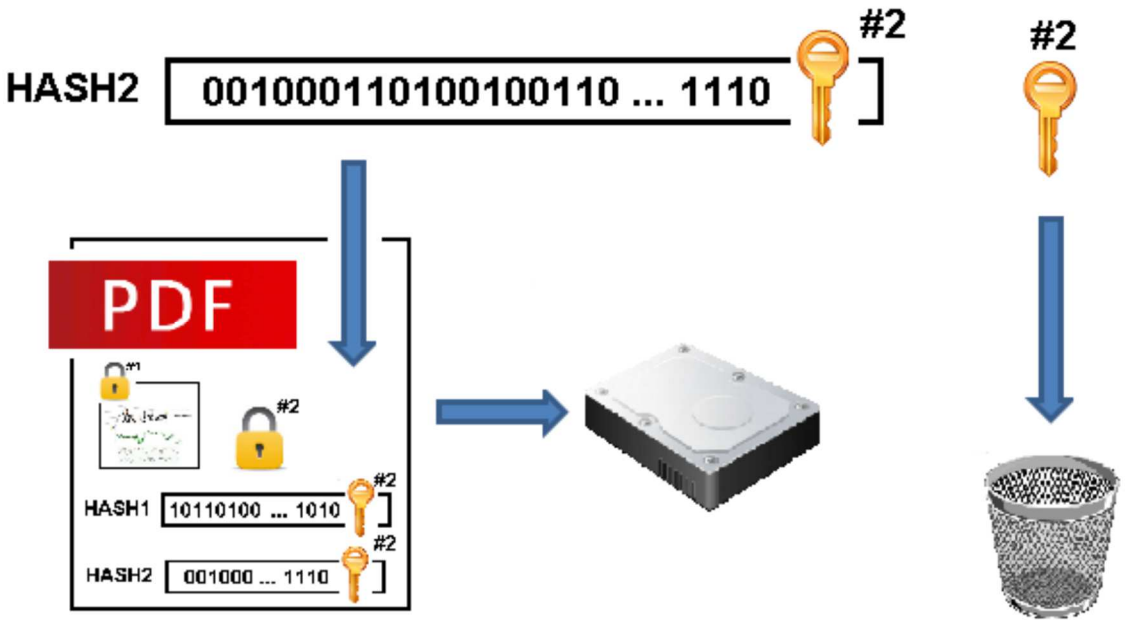
Podpisany hash oraz klucz publiczny są umieszczane w dokumencie.

2.6 Szyfrowanie dokumentu



Nowy hash dla dokumentu i zaszyfrowanych danych biometrycznych jest wyliczany poprzez zastosowanie algorytmu SHA-256.

2.7 Zapisanie dokumentu



Drugi podpisany hash jest umieszczany w dokumencie. Dokument jest zapisywany a klucz prywatny jest usuwany. W rezultacie otrzymujemy zintegrowany z danymi biometrycznymi dokument w formacie .pdf.

3 Certyfikaty

Oprogramowanie Kofax posiada następujące certyfikaty w zakresie bezpieczeństwa.


Certificate

Approved Software

SOFTPRO GmbH

SignDocWeb 4.x


Certificate

Approved App

SOFTPRO GmbH

SignDoc Mobile 2.x for Android, 2.x for iOS and 1.x for Windows RT


Certificate

Approved Software

SOFTPRO GmbH

- SignDoc 3.2