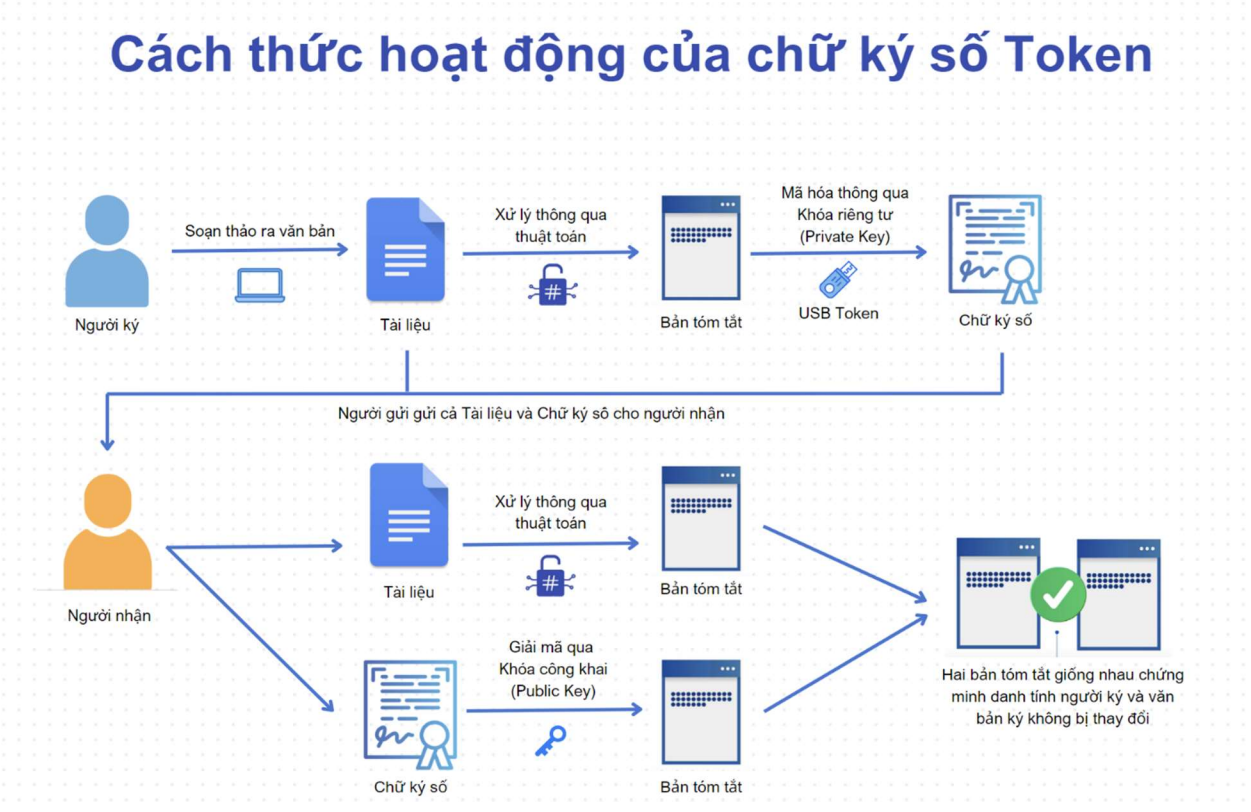
USB Token

- Sử dụng công nghệ smart card (thuộc thể loại security token) đây là loại cơ chế bảo mật hai lớp (2FA) gồm thiết bị ngoại vi kết hợp với một mã PIN xác thực để xác thực truy cập
- SmartCard được thiết kế với các mạch tích hợp IC tạo thành từ các mạch bán dẫn nhạy cảm với các hiện tượng vật lý như dòng điện, bức xạ, điện thế và tần số.
- Vấn đề bảo mật Smart Card đáp ứng
    + ***An toàn lớp vật lý:*** với kích thước nhỏ và thiết kế đa lớp, Smart Card chống được việc tấn công vật lý như quét thông qua kính hiển vi quang học, chất hóa học, lưới (đường tín hiệu) bảo vệ việc phân tích xử lý dữ liệu động; Cảm biến tín hiệu đo, biến môi trường để ngừng hoạt động chip gây nhiễu cho Attacker
    + ***An toàn lớp logic:*** SmartCard hoạt động theo cơ chế tuần tự, giao thức logic kết nối với máy tính trạm thông qua chuẩn PKCS#11 là tập hợp các hàm API phục vụ cho các thao tác mật mã với các thuộc tính "không thiết lập lại được" để bảo đảm kiểm soát chặt chẽ hoạt động của SmartCard. Do vậy mà khóa bí mật không thể truyền ra ngoài khỏi phạm vi vật lý của Smart Card
    + ***An toàn lớp thứ cấp:***
        - Mức phần cứng: cân bằng các vi mạch và giảm thiểu các phát xạ điện từ để hạ thấp tín hiệu điện thực hiện các quá trình ngẫu nhiên tương tranh nhằm làm tăng biên độ mức nhiễu. Xử lý các ngắt và tốc độ đồng hồ biến thiên được đưa vào với các nhiễu đếm thời gian để ngăn cản hoặc cản trở sự liên kết của các vết.
        - Mức phần mềm: Thực hiện sắp thứ tự quá trình ngẫu nhiên đối với các giải pháp thay thế thuật toán song song nhằm giảm thiểu các tín hiệu liên quan; Thực hiện các trễ ngẫu nhiên hay các tuyến thay thế để thêm vào nhiễu đếm thời gian, nhằm cản trở sự liên kết của các vết và làm hỏng chất lượng của vết lượng sai; Cài đặt các vận hành khóa cố định thời gian để khử những tham số phụ thuộc thời gian trong nguyên liệu khóa và tránh cho các giá trị trung gian sự phân tích dòng

điện đơn giản bằng theo dõi trực quan các vết; Thêm vào các giá trị ngẫu nhiên (sẽ được khử đi sau này) làm mù các giá trị trung gian nhằm ngăn chặn rò rỉ thông tin hữu ích. Những giá trị này được thiết kế cẩn thận để bù lại cho sự chênh lệch gây ra bởi các giá trị ngẫu nhiên.

- Mức ứng dụng: kiểm tra mã số bí mật cá nhân PIN. Mã số này bị khóa lại sau ba lần thử liên tục không thành công sẽ là sự bảo vệ hữu ích chống lại phân tích lượng sai. Việc bộc lộ đầu vào và đầu ra của các thuật toán mật mã cần phải được hạn chế hoặc giới hạn để tránh kẻ tấn công thực hiện phân tích lượng sai.



1. Người ký thông qua soạn thảo để tạo ra tài liệu cần ký số.
2. Người ký đưa tài liệu vào phần mềm ký số. Các thuật toán trong phần mềm xử lý tài liệu và biến nó thành một Bản tóm tắt. Về cơ bản, Bản tóm tắt chính là tài liệu được thể hiện bằng các ký hiệu đặc biệt, cho phép phần mềm có thể đọc và đối chiếu.

3. Người ký cắm USB Token vào máy tính. Khi này Khóa công khai lưu trữ trong USB Token sẽ thực hiện mã hóa Bản tóm tắt thành Chữ ký số.
4. Người ký gửi cả Tài liệu gốc và Chữ ký số qua cho Người nhận.
5. Người nhận sử dụng phần mềm ký số của họ để "đọc" Tài liệu nhận được và Chữ ký số. Một mặt các thuật toán trong phần mềm sẽ xử lý Tài liệu nhận được thành một Bản tóm tắt số 1. Mặt khác bằng Khóa công khai (mà người gửi chia sẻ), phần mềm sẽ giải mã Chữ ký số nhận được ra thành Bản tóm tắt số 2.
6. Phần mềm sẽ đối chiếu Bản tóm tắt số 1 và số 2 với nhau, nếu 2 bản này trùng khớp chứng tỏ danh tính của Người ký đã được xác thực và Tài liệu mà Người ký gửi sang được đảm bảo toàn vẹn giống như Tài liệu tại thời điểm ký.