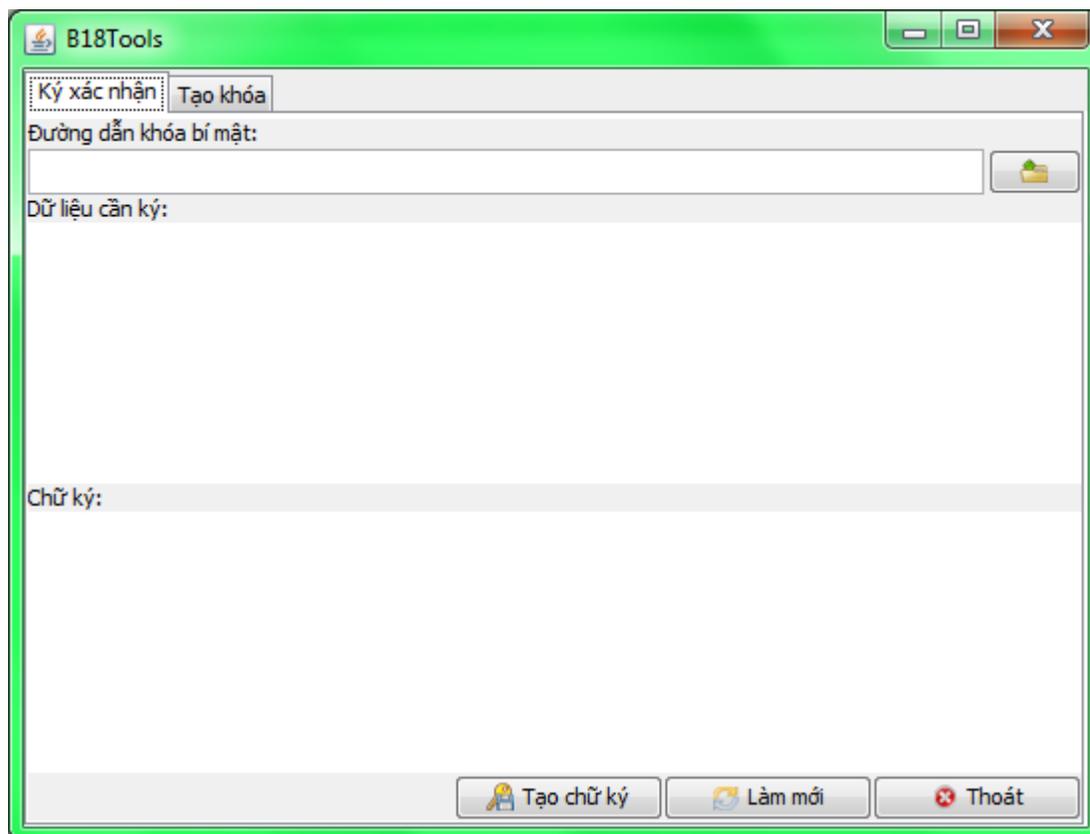


Hướng Dẫn Sử Dụng Tool P18tool



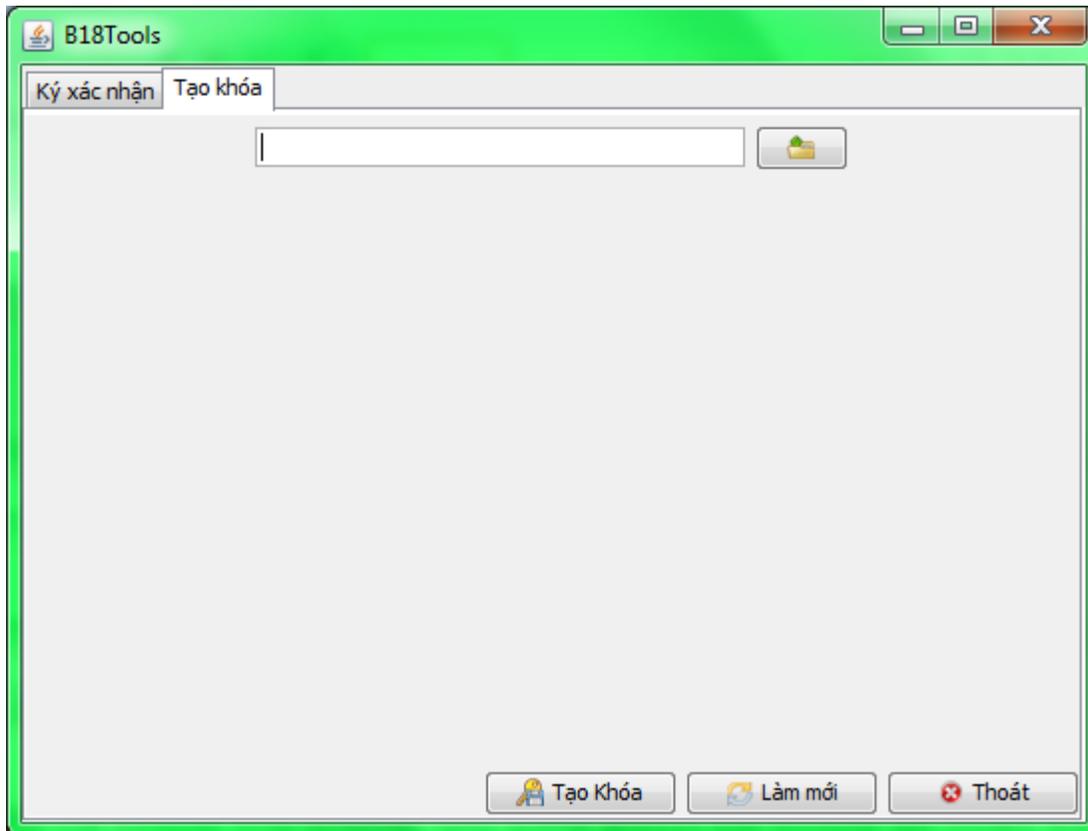
Công cụ khá đơn giản và dễ sử dụng hầu như chúng ta có thể nhìn thấy một cách trực quan các trường cụ thể của chương trình , một giao diện tiếng việt phần nào cũng góp phần vào việc giúp chúng ta có thể dễ dàng tương tác với nó.

Công cụ bao gồm hai chức năng chính là tạo ra khóa cho người dùng và tạo chữ ký khi cần ký trên một văn bản nào đó

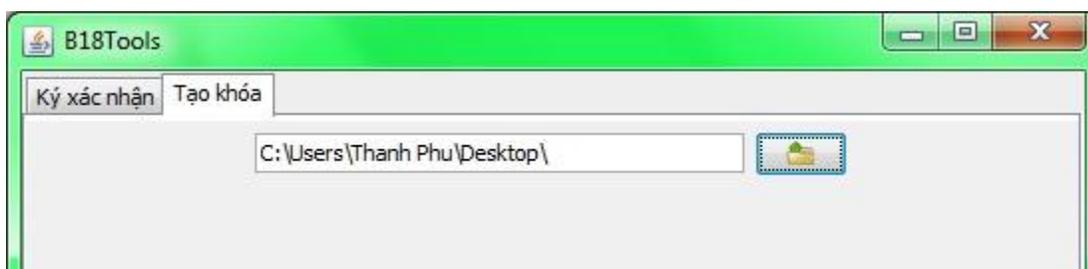
- Về chức năng tạo khóa thì trong đó bao gồm cả khóa bí mật và khóa công khai của người dùng , công cụ chỉ đơn giản tạo ra một cặp khóa, dựa vào ngày giờ của hệ thống để đặt tên cho khóa sau khi khóa được tạo ra chúng ta có thể đặt tên lại theo ý thích của chúng ta, người dùng

An toàn và Bảo mật hệ thống

chỉ việc chọn đường dẫn để lưu cập khóa mà thôi. ở công cụ này sử dụng thuật toán mã hóa bất đối xứng RSA để thể hiện với độ dài khóa được đặt cố định là 1024



ở button có biểu tượng folder chúng ta nhấp vào đấy để chỉ định đường dẫn lưu cập khóa của chúng ta , còn khung text là sao khi chúng ta chọn đường dẫn lưu khóa nó sẽ hiện cho chúng ta đường dẫn ra cho chúng ta thấy .



An toàn và Bảo mật hệ thống

nếu chúng không chọn đường dẫn để lưu khóa thì khóa vẫn được tạo ra khi bạn nhấp “tạo khóa” chúng được đặt định để ở ổ đĩa C của chúng ta. Khi nhấn nút “tạo khóa” thì quá trình tạo khóa được bắt đầu chúng ta đợi khoảng 10 giây thì chương trình sẽ hiện ra một bản thông báo nói cho chúng ta biết là khóa đã được tạo thành công



Đến đây bạn đã có được cặp khóa cho mình rồi

Vì khóa được đặt tên theo nguyên tắc lấy thời gian của hệ thống hiện tại của bạn nên tên của nó sẽ là một dãy số rồi tới “_private.key” nếu là khóa bí mật , tới “_public.key” nếu là khóa công khai.

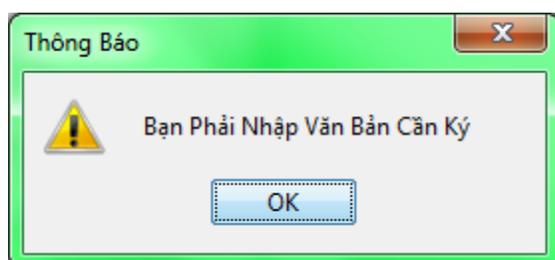
Nếu trong quá trình bạn chọn thư mục để lưu rồi mà muốn đổi sang thư mục khác bạn có thể nhấp vào biểu tượng folder để chọn thư mục lưu khác hay bạn cũng có thể nhấp vào nút “Làm mới” để mọi thứ điều trở lại từ đầu trước khi chọn, hay bạn không muốn tạo khóa nữa thì bạn cũng có thể nhấp nút “hủy” để thoát khỏi chương trình không tạo nữa.

Về chức năng Ký xác nhận : ở khung đường dẫn khóa bí mật bạn nhấp vào biểu tượng folder để duyệt tìm đến nơi để khóa bí mật của mình vào để tiến hành ký ,khung text cạnh đó là để thể hiện đường dẫn khóa bí mật sau khi bạn chọn. nếu như bạn không chọn khóa bí mật mà nhấn vào “tạo chữ ký “ thì không thể ký được chương trình sẽ hiện ra một bản thông báo yêu cầu bạn phải nhập vào “key private” bạn nhấp ok rồi chọn khóa bí mật để nhập vào .

An toàn và Bảo mật hệ thống



Khi nhập xong khóa bí mật ở khung dữ liệu cần ký chúng ta nhập vào văn bản mà bạn cần ký xác nhận ,bạn có thể copy rồi paste vào trong khung .nếu như bạn không nhập vào nội dung cần ký mà nhấp vào “tạo chữ ký “ thì bạn cũng không thể tạo được chữ ký ,khi đó chương trình sẽ xuất ra cho bạn một bản thông báo yêu cầu bạn phải nhập vào nội dung cần ký , bạn nhấp ok rồi tiến hành nhập vào nội dung cần ký là được .

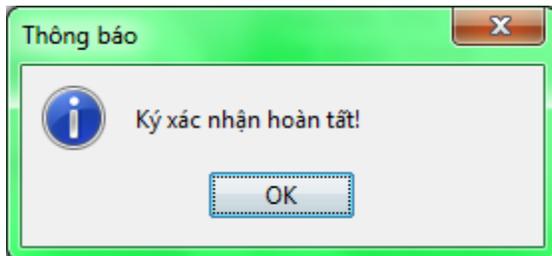


Chú ý: khi ban đầu vào nếu bạn không nhập nội dung ký , không nhập khóa bí mật vào thì chương trình vẫn hiện ra bản thông báo yêu cầu bạn nhập vào nội dung cần ký chứ không phải là nhập vào khóa bí mật trước như bố cục sắp xếp của chương trình ,vì bạn phải ký trên cái gì trước thì bạn mới cần khóa để ký.

Ở khung chữ ký bạn không nhập gì vào trong khung này cả, mà khung này dùng để thể hiện chữ kí của bạn sau khi bạn đã ký lên văn bản ban đầu,cho dù bạn có ghi gì vào đó cũng không có ý nghĩa vì sau khi ký thì nó cũng được xóa sạch để thay vào đó là chữ ký ở dạng plaintext.

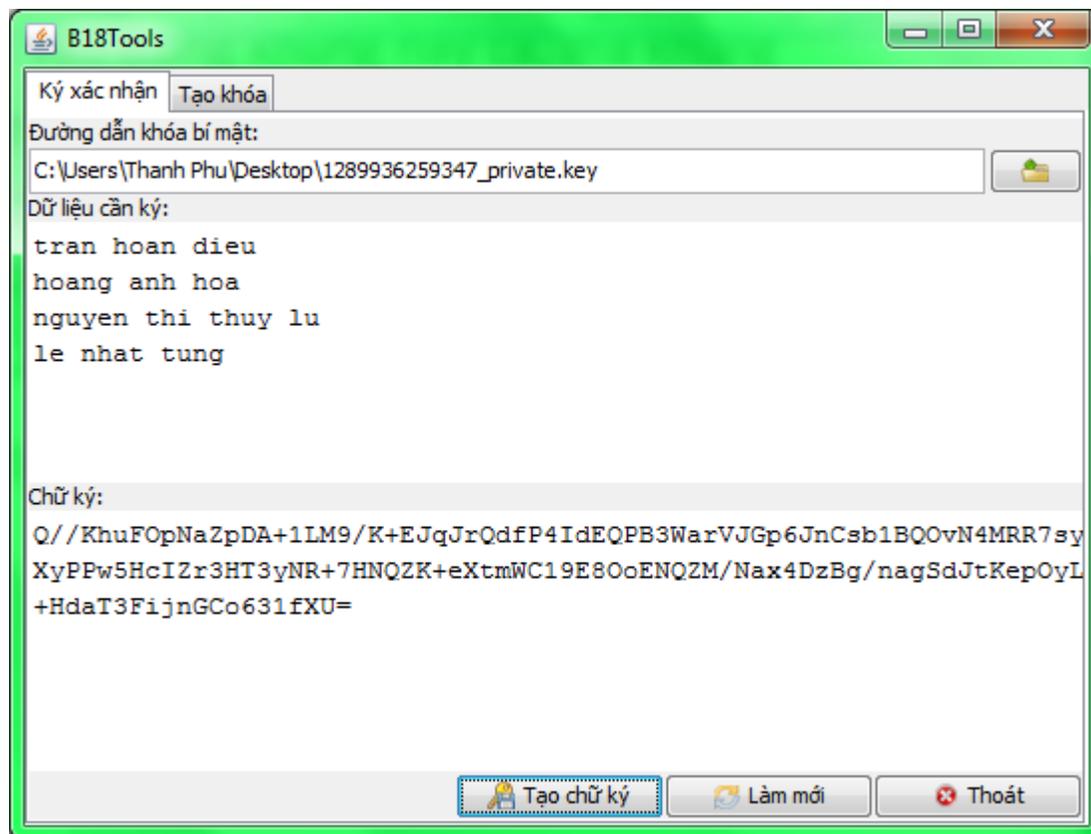
An toàn và Bảo mật hệ thống

Khi bạn nhấp vào nút “Tạo chữ ký” thì quá trình ký bắt đầu khoảng 10 giây sau chương trình sẽ hiện cho bạn một bản thông báo nói rằng bạn đã ký thành công



Lúc này ở khung “ chữ ký “ sẽ xuất hiện một đoạn text đó chính là chữ ký được tạo ra trên dữ liệu bạn nhập vào và khóa bí mật .bạn có thể copy đoạn chữ ký này để xác thực , đồng thời khi tạo ra chữ ký dạng text hiện ra tại giao diện chương trình này thì chương trình còn tạo ra cho chúng ta một file chữ ký nằm cùng thư mục với thư mục chứa khóa bí mật mà bạn vừa nhập vào . file nào cũng được đặt tên dựa trên nguyên tắc lấy ngày giờ của hệ thống giống như khi tạo khóa . file này có phần mở rộng là “ .sign “ bạn có thể dùng file này để tạo xác thực thay cho đoạn text trong chương trình cũng được .

An toàn và Bảo mật hệ thống



Hai nút còn lại chức năng đã được giới thiệu bên thẻ tạo khóa bên kia có lẽ không cần nhắc lại

Hy vọng các bạn có thể sử dụng được một cách dễ dàng sau khi đọc bài hướng dẫn của mình :D