



## GIẢI PHÁP MÃ HÓA CẤP CAO DÀNH CHO DOANH NGHIỆP

Tuyên ngôn về sứ mệnh:

*“Users should Live and Work in a Globally-Encrypted Environment”  
(Chúng ta nên Sống và Làm việc trong Môi trường được Mã hóa Toàn cầu)*

# Diễn giả



Serge Binet

Co-founder, PRIM X TECHNOLOGIES

## Diễn giả:

Ông Serge Binet

*Đồng sáng lập Công ty Công nghệ Prim'X*

*DOB: 1965*

## Mục tiêu của Prim'X:

Mục tiêu của PRIM'X là giới thiệu một cách thức mới để tích hợp mã hóa trong một tổ chức nhằm bảo vệ tốt hơn các dữ liệu nhạy cảm khỏi bị mất, đánh cắp, tiết lộ và gián điệp kinh tế. Vì những lý do này, các tổ chức cần phải thực hiện một chính sách toàn cầu “Mã hóa mọi thứ, mọi nơi và mọi lúc”

## Tầm nhìn của PRIM'X cho mã hóa là phải :

Toàn diện – Đơn giản – Trong suốt – Tự động và Chi phối bởi các chính sách an ninh

# NỘI DUNG



## ■ PHẦN I. Giới thiệu về Prim'X

- Giới thiệu
- Khách hàng & Tham chiếu

## ■ PHẦN II. Tầm nhìn và Sứ mệnh

- Tầm nhìn
- Các trường hợp sử dụng chính

## ■ PHẦN III. Giải pháp

- Tổng quan
- Cryhod, ZoneCentral, Zed, ZedMail và các giải pháp khác
- Đối tượng khách hàng chính

# I.1/ PRIM'X – GIỚI THIỆU



- Là Công ty của Pháp, thành lập năm 2003, cung cấp dịch vụ Chính sửa phần mềm chuyên về An ninh mạng (**CyberSecurity**), cụ thể là lĩnh vực mã hóa
- Văn phòng đặt tại Paris (Kinh doanh) và Lyon (Trụ sở chính & Lab)
- Đối tác kinh doanh và triển khai tại Việt Nam: **MKgroup**
- Các sản phẩm phần mềm được thiết kế hướng đến đối tượng khách hàng trung bình – lớn – rất lớn và Cơ quan hành chính công / Chính phủ với + **1,5 triệu người dùng** chủ yếu tại Pháp/Châu Âu
- Các giải pháp của Prim'X đã được nghiên cứu và thử nghiệm bởi:



COMMON CRITERIA  
CERTIFIED  
EAL3+



FRANCE  
CyberSecurity  
Label



EU-Restricted



Bundesamt  
für Sicherheit in der  
Informationstechnik

German  
Federal Office  
Security



NATO-Restricted

## 1.2/ Khách hàng



- Các nhà sản xuất công nghiệp (THALES, RENAULT, SAFRAN, DASSAULT, CNES, ASL...)
- Các cơ sở hạ tầng quan trọng (Lĩnh vực hạt nhân, Cấp điện/nước, Nhà máy, Cơ quan Nhà nước...)
- Tất cả các lĩnh vực:
  - Ngân hàng (CREDIT AGRICOLE, SOCIETE GENERALE, ...)
  - Viễn thông (ORANGE, BYTEL, INWI)
  - Giao thông (Đường sắt, Cảng, Sân bay, ...)
  - Y tế (Bệnh viện, Các cơ sở Y tế Quốc gia)
- Cơ quan Hành chính và Chính phủ:
  - Ủy ban Châu Âu
  - Các bộ ngành trọng yếu (Cơ quan chính phủ, Bộ nội vụ, Bộ quốc phòng, Bộ tư pháp)
  - Tháng 01/2016: Cấp phép sử dụng cho TOÀN BỘ CƠ QUAN NHÀ NƯỚC CỦA PHÁP
    - Khách hàng tham chiếu chính: ANSSI (Cơ quan An ninh Quốc gia Pháp), Bộ nội vụ & Quốc phòng
  - Tháng 01/2017: Phần mềm Zed! được sử dụng cho CHÍNH PHỦ LIÊN MINH CHÂU ÂU

## II.1/ TẦM NHÌN / Tóm lược



- Một **CÁCH THỨC MỚI** để tích hợp mã hóa trong các tổ chức:
  - *Mã hóa... Mọi thứ, Mọi nơi và... Mọi lúc*
- Để đạt được mục tiêu đó, Mã hóa phải:
  - *Toàn diện*
  - *Đơn giản*
  - *Trong suốt và liền mạch*
  - *Tự động*
  - *Chính sách Bảo mật được tuân thủ*

## II.1/ Tầm nhìn / ...Mã hóa và Bảo mật



- Mã hóa:
  - Là biện pháp phòng vệ an ninh mạng chống **trộm cắp, mất dữ liệu, tiết lộ thông tin, gián điệp kinh tế & công nghiệp & chính trị & xuyên quốc gia**
  - Là biện pháp bảo vệ **BỊ ĐỘNG (PASSIVE) cuối cùng**, luôn hoạt động khi các biện pháp bảo vệ chủ động đã bị phá vỡ
  - **Cho phép Quản lý Quyền được biết (Need-to-Know)**, cho phép mã hóa phân tách **nội bộ**, bằng cách phân tách giữa:
    - Tôi và nhân viên của tôi, đồng nghiệp và các nhân viên tạm thời
    - Nhóm của tôi và các nhóm khác
    - Phòng của tôi và phòng CNTT
    - Tổ chức của tôi và các nguồn lực khác
    - Tôi / nhóm của tôi / phòng của tôi / tổ chức của tôi và “*thế giới bên ngoài*”
- **Tuân thủ** các quy tắc kinh doanh & luật doanh nghiệp
- Phải được áp dụng trên các tệp cục bộ, toàn bộ thư mục, Windows, nội dung chia sẻ trên máy chủ, NAS, thư viện MS Sharepoint™, thư mục dự phòng, ổ đĩa USB, bộ lưu trữ Cloud, email...

## II.2/ Trường hợp sử dụng chính



- Giải pháp mã hóa cấp cao PRIM'X dành cho:
  - Giải quyết các nhu cầu mở rộng khác nhau →
  - Với cùng một mức độ quản lý và giao diện như nhau
    - tác động với người dùng,
    - tác động với CNTT,
    - tác động với CISO,
  - Phương pháp mã hóa tiên tiến (AES256, RSA 2/4k)
  - Tương thích với hầu hết PKI và thẻ thông minh (tùy chọn)

Bảo vệ toàn bộ cơ sở hạ tầng CNTT

Quản lý quyền được biết, bảo vệ nội dung chia sẻ, phân tách an ninh khỏi bộ phận CNTT, phân tách thông tin trong nội bộ

Bảo vệ toàn diện máy tính xách tay và ổ đĩa (chống trộm)

Bảo vệ email (nội bộ VÀ bên ngoài)

Trao đổi thông tin mật với bên thứ ba

Bảo mật phương tiện lưu trữ di động

Cung cấp an ninh khi đi lại, chuyển vùng

Bảo đảm Tính tuân thủ

Bảo vệ dữ liệu của khách hàng

Bảo vệ dữ liệu trên Cloud (bộ lưu trữ cloud, đĩa VM) \*\*Q4/2017

V.V...



# III./ Tổng quan về các giải pháp

Mục tiêu/Nhu cầu	Giải pháp
Ổ đĩa, máy tính xách tay, các phương tiện có thể tháo rời cần bảo vệ vòng ngoài	Cryhod
Môi trường của người dùng (Windows, các khu vực dữ liệu, thư mục chủ, ổ đĩa gắn trên mạng, ..., phân tách theo người dùng)	ZoneCentral
Nội dung chia sẻ trên mạng (máy chủ tập tin, NAS, SAN) và Quản lý Quyền được biết (Need-to-Know)	ZoneCentral
Trao đổi dữ liệu và email	Zed / ZedMail ZoneCentral
Thư viện tài liệu MS Sharepoint™	ZonePoint
Môi trường người dùng trên điện toán đám mây (OneDrive™)	Orizon (Q4/2017)
Kho lưu trữ và trung tâm dữ liệu dự án trên điện toán đám mây	Orizon (Q4/2017)

- **Chống trộm** cho máy tính xách tay và ổ đĩa di động
- Mã hóa bề mặt ở mức **phân vùng Sector** (Partition's sector level)
- Phân vùng của hệ thống có thể được mã hóa
- Xác thực **trước khi khởi động**
- Hỗ trợ **UEFI** và firmware BIOS

Các trường hợp sử dụng phổ biến: nhóm máy tính xách tay / máy tính bảng chuyên nghiệp đã được chống va chạm / tuân thủ



Cryhod authentication (customizable)

Workstation  
starts or  
wakes-up



OS starts



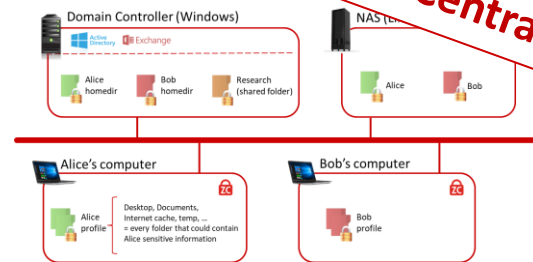
Entering the user key  
(password, RSA key-file, smartcard)



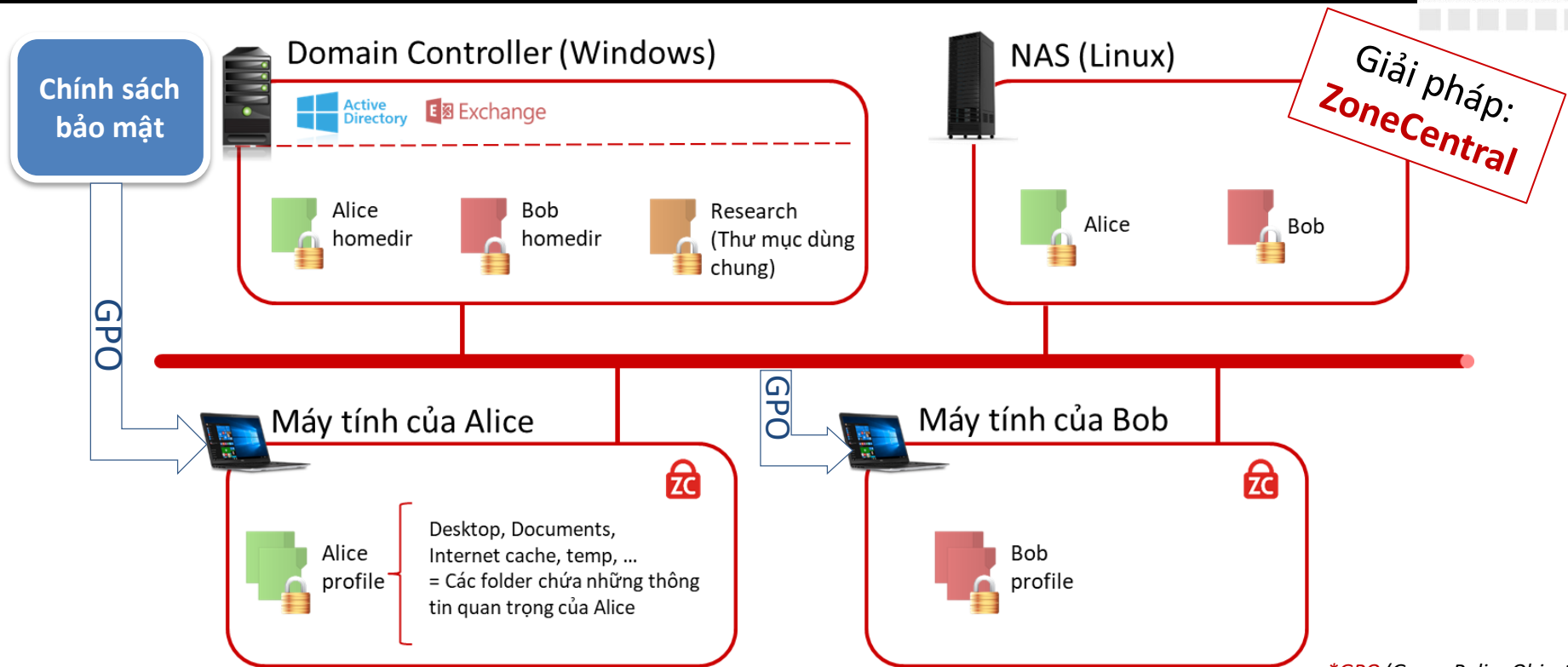
# ZoneCentral /Mã hóa mức độ tệp

CORPORATE ENCRYPTION SYSTEMS

- Bảo vệ **toàn bộ môi trường làm việc** của người dùng (trạm làm việc và các khu vực mở rộng)
  - Bảo vệ **nội dung chia sẻ** trên mạng nội bộ
  - Quản lý **Quyền được biết**
- 
- Mã hóa ở “mức độ hệ thống tệp” (tệp, thư mục) thực sự mạnh mẽ:
    - **Ngay lập tức**, không chịu tác động của người dùng
    - **Không thay đổi** cách thức làm việc của người dùng, không thay đổi đối với CNTT!
    - Có thể áp dụng cho **bất kỳ** hệ thống tệp nào được hiển thị trong Windows: nội bộ, USB, mạng, DFS, SAN/NAS
    - Các khu vực mã hóa có thể được xác định theo Chính sách bảo mật (mã hóa “**có quản lý**”) chẳng hạn như hồ sơ Windows, thư mục My Documents ...
    - Đồng bộ hóa với các nhóm AD
    - Cho phép mã hóa liên tục đến **các tệp dự phòng**, với các khóa (key) do người dùng đặt!



# ZoneCentral / Bảo vệ toàn bộ môi trường làm việc



\*GPO (Group Policy Objects)



# Zed!

## /Mã hóa để trao đổi thông tin



Container.zed

- **“Cặp ngoại giao” (Diplomatic bag) để trao đổi file dữ liệu**
  - Trở thành một Tiêu chuẩn rất phổ biến tại Pháp (và tại Châu Âu – qua Chính phủ EU)
  - Được Cơ quan an ninh thông tin và mạng lưới Pháp (ANSSI) chính thức công bố khuyến nghị sử dụng khi trao đổi file dữ liệu quan trọng

- Hỗ trợ các hệ điều hành phổ biến:



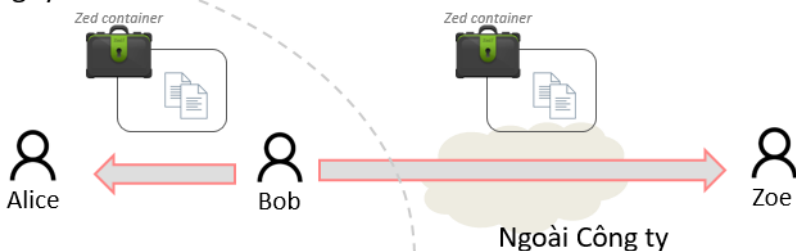
iOS



- Phiên bản miễn phí: Zed! Free

- Tại địa chỉ: <https://www.zedencrypt.com>
- Người nhận có thể đọc và chỉnh sửa thông tin được mã hóa (Encrypted container)
- Và trả lời với file mã hóa được chỉnh sửa với cùng một quyền truy cập

Trong Công ty





# Zed Mail /Mã hóa Thư điện tử/Email



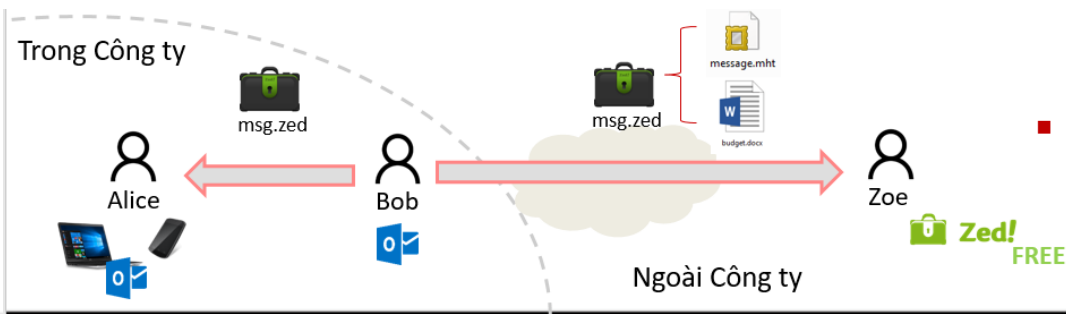
- **Áp dụng mã hóa thư điện tử nội bộ và cho phép mã hóa thư gửi ra bên ngoài**

- Mở rộng phạm vi mã hóa thư điện tử cùng với hạ tầng PKI
- Cho phép thư mã hóa đọc được ở mọi nơi
  - Webmails, điện thoại thông minh, máy tính bảng và máy tính cá nhân

- **Tích hợp plug-in với MS Outlook™** (hỗ trợ tất cả các phiên bản)

- File mã hóa ZED có thể đọc và gửi lại được trên mọi môi trường thông qua ứng dụng miễn phí ZED Free: Môi trường Windows, Mac, Linux, iOS, Android...
- Mã hóa có thể bắt buộc tuân thủ theo chính sách bảo mật.

- Có thể sử dụng Chữ ký số **PKI** (AD, LDAP...) và mật khẩu định trước cho gửi nhận



## III.3/ Các dự án tham chiếu



Thông tin về các dự án, trường hợp sử dụng, mục tiêu và hạ tầng, v.v được cung cấp

Thông tin chi tiết được cung cấp trong **Tài liệu Giới thiệu PRIM'X**

Hồ sơ y tế của bệnh nhân	Khu phức hợp Bệnh viện lớn với hệ thống hạ tầng <b>CITRIX</b>
Hạ tầng sân bay	Tăng cường bảo mật của <b>Hệ thống thông tin</b>
Cơ quan Chính phủ	Bảo vệ các thông tin mật của Chính phủ Pháp trong quá trình lưu chuyển
Tập đoàn Công nghiệp Quốc phòng	Áp dụng chính sách bảo mật tại các máy trạm
Nhà máy hạt nhân lớn của Pháp	Bảo vệ môi trường tương tác trên MS <b>Sharepoint</b> ™
Bộ Nội vụ Pháp	Mã hóa lớn cho toàn bộ mạng lưới của Bộ Nội vụ Pháp ( <b>với trên 120,000</b> máy tính)
Hãng sản xuất xe	Bảo vệ dữ liệu nhạy cảm tại các Trung tâm R&D

Các dự án trong lĩnh vực Ngân hàng và Viễn thông sẽ được bổ sung



**TRÂN TRỌNG CẢM ƠN!**