

# PRIMEKEY SOLUTIONS AB

## INNOVATIVE SOFTWARE NETWORKING CONFERENCE

Admir Abdurahmanovic  
VP, co-founder

2013-02-21

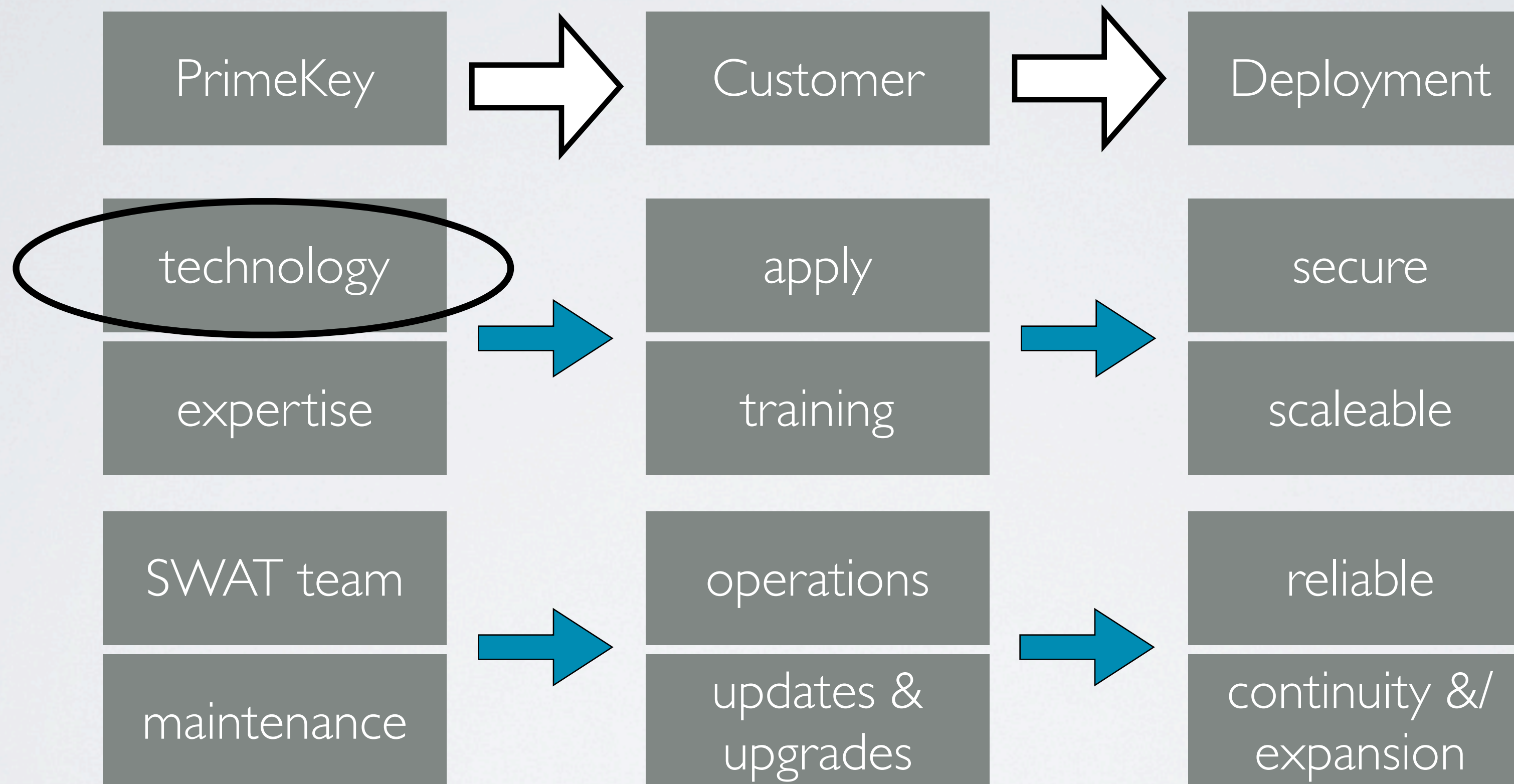
# PRIMEKEY AT A GLANCE

- Solutions and Professional Services in area of Applied Cryptography with focus on PKI
- Customers are Governments & Large Enterprises
- SME with headquarters in Stockholm, Sweden, 2012 opened subsidiary in Aachen/Germany
- Developers and commercial force behind EJBICA.org and SignServer.org
- Open Standards, Open Source
- Active in more than 40 countries
- Organic growth, 20-30% per year



The screenshot shows the PrimeKey website homepage. At the top, there is a navigation bar with links for Home, Get Support, Sitemap, Share, and FOLLOW US ON twitter. Below this is a secondary navigation bar with links for Products, Solutions, Services, News, Partners, Community, Company, and Contact us! The main content area features a large banner for 'Adaptable enterprise PKI & digital signature solutions' with a sub-header 'Reliable first-hand skills, support & services'. To the left of this banner is a photo of two men in a meeting, with text overlaying it: 'next training course EJBICA PKI BY PRIMEKEY'. Below the main banner is a section titled 'The very 1st Common Criteria Certified Open Source PKI Solution...' with a list of 5 points and a link to 'Read more about the CESeCore project'. At the bottom, there are four columns of content: 'Free PKI booklet!', 'Events' (listing various conferences and seminars), 'Releases' (listing software versions and dates), and 'Products & Solutions' (highlighting the CESeCore project). The footer contains copyright information for PrimeKey Solutions AB and contact details.

# HOW WE WORK?



# OPEN STANDARDS

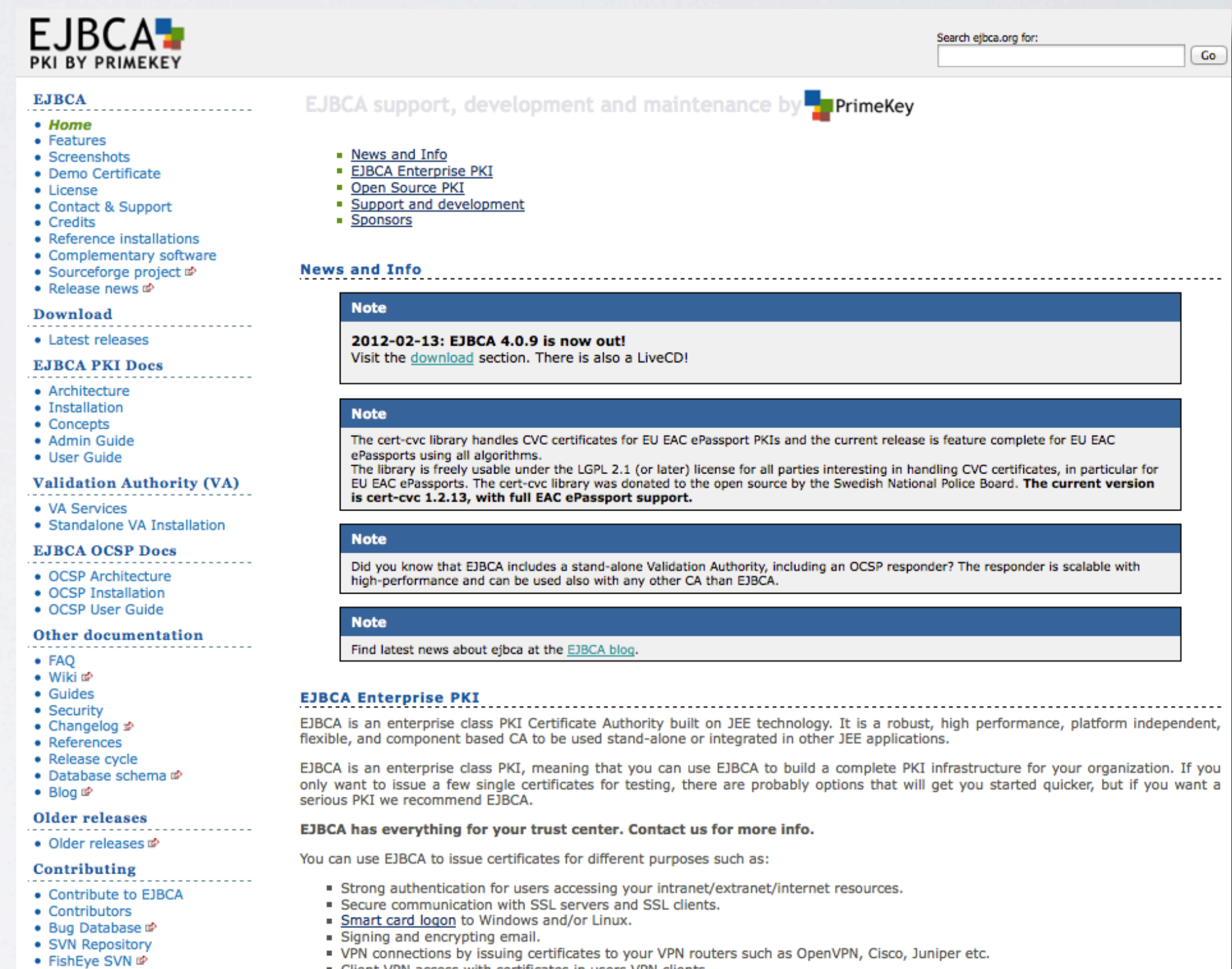
- PrimeKey uses tested, approved, standardized technologies
- Open Standards advantages:
  - easier integration with other applications
  - longer and healthier life-cycle
  - lower total cost of ownership
- Open Standards bring interoperability with other related technologies (databases, directories, application servers, HSMs)
- Our solutions are platform-neutral (Windows, Unix, Linux, OSX)

# TECHNOLOGY/R&D

## EJBCA - PKI BY PRIMEKEY

**E**nterprise **J**ava **B**eans **C**ertificate **A**uthority

- Leading PKI world wide, thousands of deployments
- Full blown, industrial strength
- Government & Law Enforcement, eID/ePassports, Banking/Finance, IT/telecom, Service Providers



**EJBCA**  
PKI BY PRIMEKEY

Search ejbca.org for:  Go

**EJBCA**

- [Home](#)
- [Features](#)
- [Screenshots](#)
- [Demo Certificate](#)
- [License](#)
- [Contact & Support](#)
- [Credits](#)
- [Reference installations](#)
- [Complementary software](#)
- [Sourceforge project](#)
- [Release news](#)

**Download**

- [Latest releases](#)

**EJBCA PKI Docs**

- [Architecture](#)
- [Installation](#)
- [Concepts](#)
- [Admin Guide](#)
- [User Guide](#)

**Validation Authority (VA)**

- [VA Services](#)
- [Standalone VA Installation](#)

**EJBCA OCSP Docs**

- [OCSP Architecture](#)
- [OCSP Installation](#)
- [OCSP User Guide](#)

**Other documentation**


- [FAQ](#)
- [Wiki](#)
- [Guides](#)
- [Security](#)
- [Changelog](#)
- [References](#)
- [Release cycle](#)
- [Database schema](#)
- [Blog](#)

**Older releases**

- [Older releases](#)

**Contributing**

- [Contribute to EJBCA](#)
- [Contributors](#)
- [Bug Database](#)
- [SVN Repository](#)
- [FishEye SVN](#)

EJBCA support, development and maintenance by  PrimeKey

- [News and Info](#)
- [EJBCA Enterprise PKI](#)
- [Open Source PKI](#)
- [Support and development](#)
- [Sponsors](#)

**News and Info**

**Note**

**2012-02-13: EJBCA 4.0.9 is now out!**  
Visit the [download](#) section. There is also a LiveCD!

**Note**

The cert-cvc library handles CVC certificates for EU EAC ePassport PKIs and the current release is feature complete for EU EAC ePassports using all algorithms.  
The library is freely usable under the LGPL 2.1 (or later) license for all parties interesting in handling CVC certificates, in particular for EU EAC ePassports. The cert-cvc library was donated to the open source by the Swedish National Police Board. **The current version is cert-cvc 1.2.13, with full EAC ePassport support.**

**Note**

Did you know that EJBCA includes a stand-alone Validation Authority, including an OCSP responder? The responder is scalable with high-performance and can be used also with any other CA than EJBCA.

**Note**

Find latest news about ejbca at the [EJBCA blog](#).

**EJBCA Enterprise PKI**

EJBCA is an enterprise class PKI Certificate Authority built on JEE technology. It is a robust, high performance, platform independent, flexible, and component based CA to be used stand-alone or integrated in other JEE applications.

EJBCA is an enterprise class PKI, meaning that you can use EJBCA to build a complete PKI infrastructure for your organization. If you only want to issue a few single certificates for testing, there are probably options that will get you started quicker, but if you want a serious PKI we recommend EJBCA.

**EJBCA has everything for your trust center. Contact us for more info.**

You can use EJBCA to issue certificates for different purposes such as:

- Strong authentication for users accessing your intranet/extranet/internet resources.
- Secure communication with SSL servers and SSL clients.
- [Smart card logon](#) to Windows and/or Linux.
- Signing and encrypting email.
- VPN connections by issuing certificates to your VPN routers such as OpenVPN, Cisco, Juniper etc.
- Client VPN access with certificates in users VPN clients.

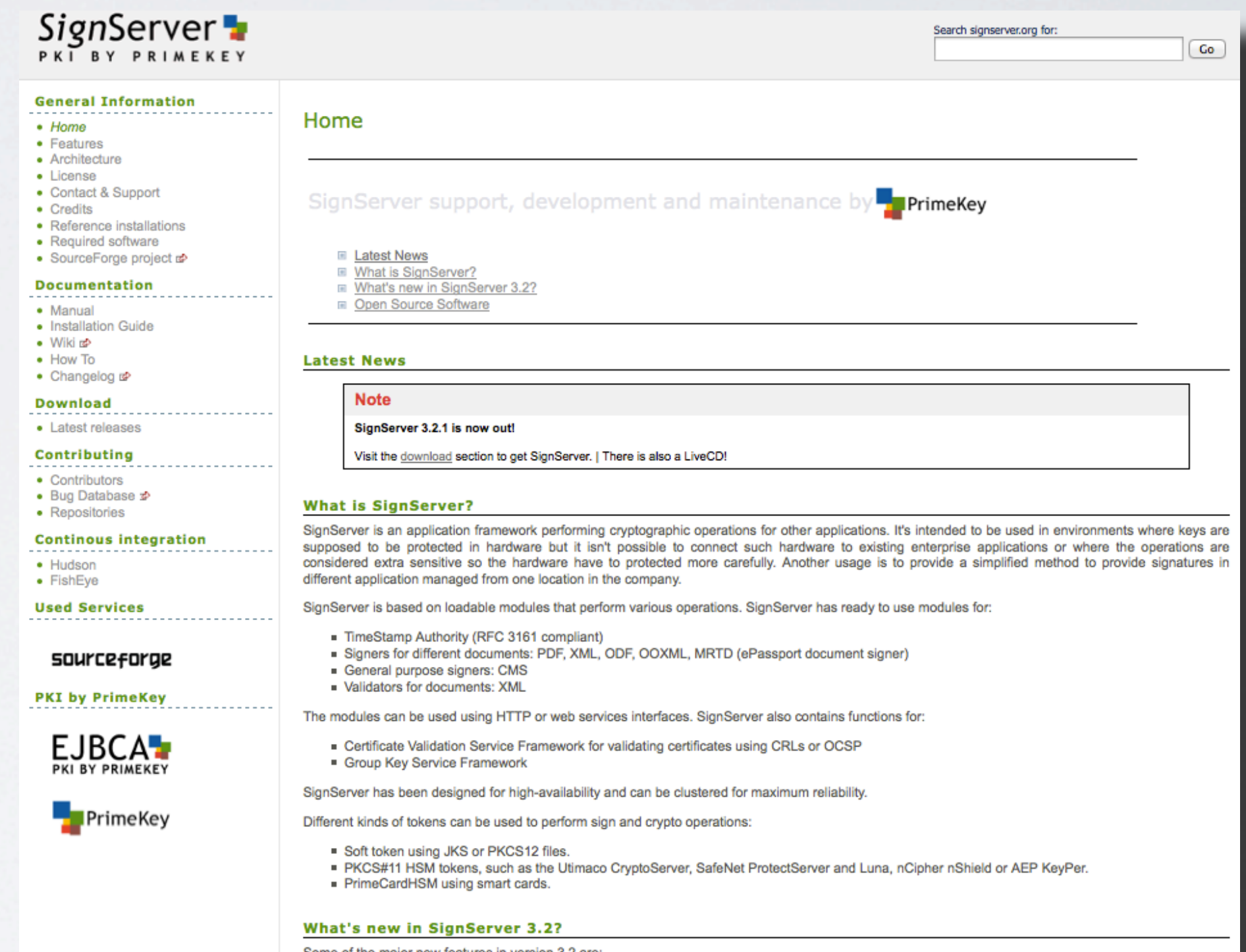
www.ejbca.org

# TECHNOLOGY/R&D

## SIGNSERVER - PKI BY PRIMEKEY

The SignServer at glance:

- Flexible framework for server-side cryptographic operations
- Document signing (PDF, XML, ODF, OOXML), ePassport, email, Time Stamps, product authenticity



The screenshot shows the SignServer website homepage. The header includes the SignServer logo and a search bar. The main content area is divided into several sections: 'General Information' with links to Home, Features, Architecture, License, Contact & Support, Credits, Reference installations, Required software, and SourceForge project; 'Documentation' with links to Manual, Installation Guide, Wiki, How To, and Changelog; 'Download' with a link to Latest releases; 'Contributing' with links to Contributors, Bug Database, and Repositories; 'Continuous integration' with links to Hudson and FishEye; and 'Used Services'. Below these are logos for SourceForge, EJBICA, and PrimeKey. The main content area features a 'Home' section with a PrimeKey logo and a 'Latest News' section with a 'Note' box stating 'SignServer 3.2.1 is now out!'. There is also a 'What is SignServer?' section with a detailed description of the application framework and its capabilities.

www.signserver.org

# TECHNOLOGY/R&D

## CESECORE

- **Certified Security Core**
- EUREKA Eurostars funded project
- Aimed to:
  - Produce an **open source** (LGPL) security core product and to have it evaluated according to Common Criteria **EAL4+**
  - Promote the integration of the security core into real-life products
- PrimeKey was project lead, three partners from Norway, Portugal and Turkey
- Project successfully finished, including Common Criteria EAL 4+ certification





Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

**CERTIFICAT ANSSI-CC-2012/33**

Ce certificat est associé au rapport de certification ANSSI-CC-2012/33

**Produit CESeCore version 1.1.2**

Développeur : CESeCore Consortium

**Critères Communs version 3.1 révision 3**

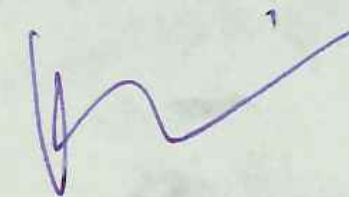
**EAL4 Augmenté**  
(ALC\_FLR.2)

**Commanditaire : CESeCore Consortium**  
**Centre d'évaluation : Oppida**

Paris, le

**14 JUIN 2012**

Le directeur général de l'agence nationale de la sécurité des systèmes d'information  
Patrick Pailloux



*Dans le cadre du CCRA, le produit est reconnu au niveau EAL4.  
Dans le cadre du SOG-IS, le produit est reconnu au niveau EAL4.*

*Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.*  
Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

# TECHNOLOGY/R&D

## CESECORE

- ✓ create electronic signatures
- ✓ validate electronic signatures
- ✓ create digital certificates and CRLs
- ✓ protect the integrity of data
- ✓ secure audit logs
- ✓ handle authentication and authorization
- ✓ handle key management

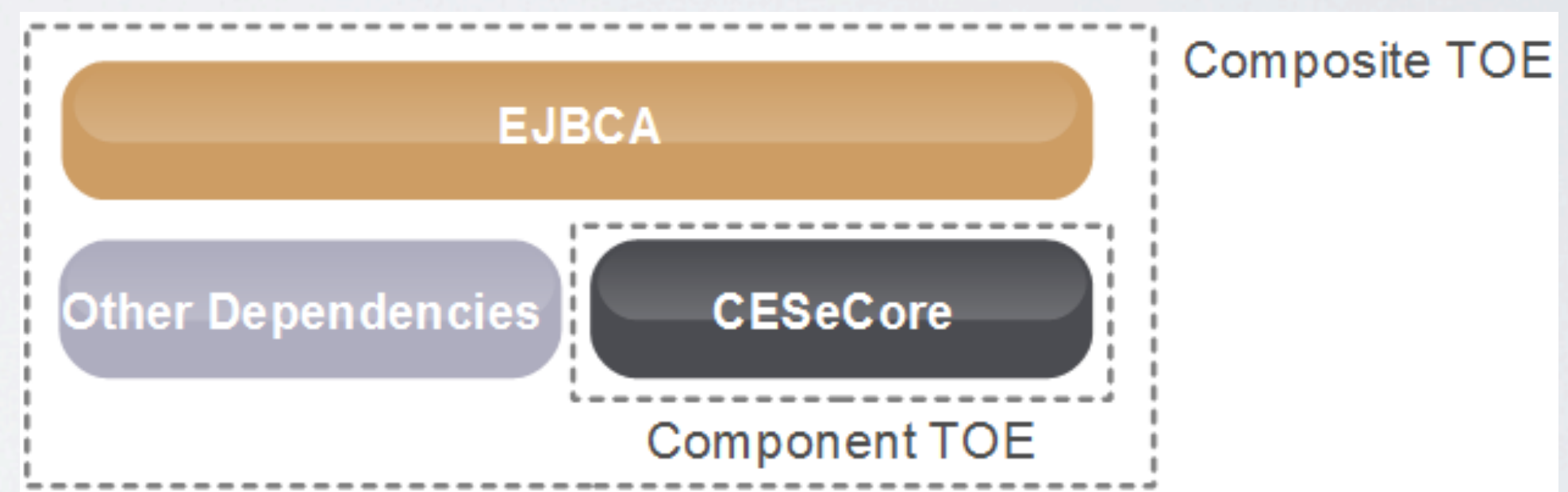
# CESeCORE FOSTERS COMMON CRITERIA EVALUATION OF RELYING PRODUCTS

Example: EJBCA is now also CC EAL 4+ evaluated, as a *composite* TOE, relying on CESeCore as a *component* TOE

CESeCore provides most of the security functions

EJBCA builds on with more functions, business logic, GUI, etc.

Tremendous time & resource savings





PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

**CERTIFICAT ANSSI-CC-2012/47**  
Ce certificat est associé au rapport de certification ANSSI-CC-2012/47

**EJBCA version 5.0.4**

Développeur : PrimeKey Solutions AB

**Critères Communs version 3.1 révision 3**

**EAL4 Augmenté**  
(ALC\_FLR.2)

conforme au profil de protection [PP-CIMC] « Certificate Issuing and Management Components Family of Protection Profiles Security Level 3 »

**Commanditaire : PrimeKey Solutions AB**  
**Centre d'évaluation : Oppida**

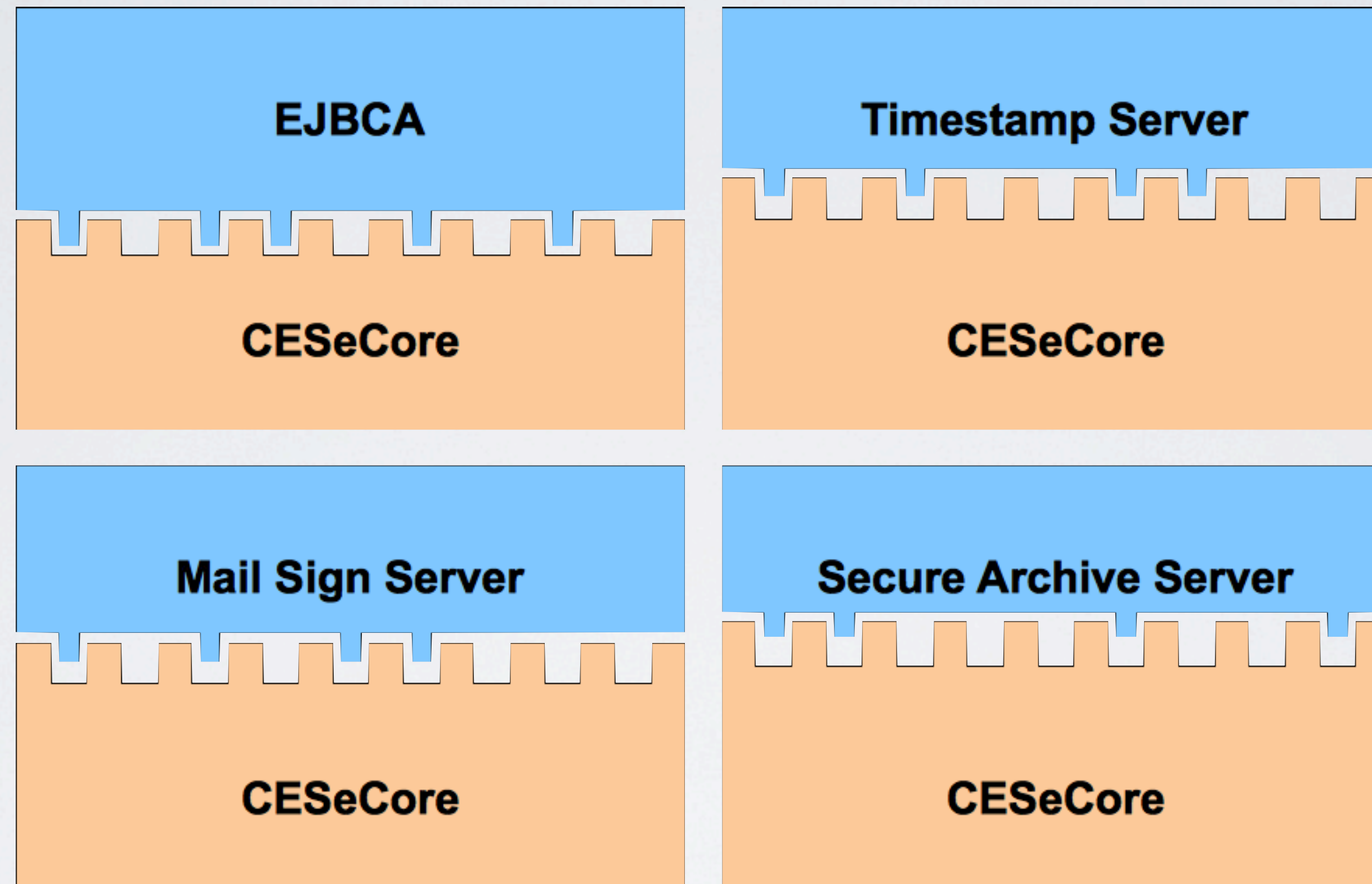
Paris, le **04 OCT. 2012**

Le directeur général de l'agence nationale de la sécurité des systèmes d'information  
Patrick Pailloux

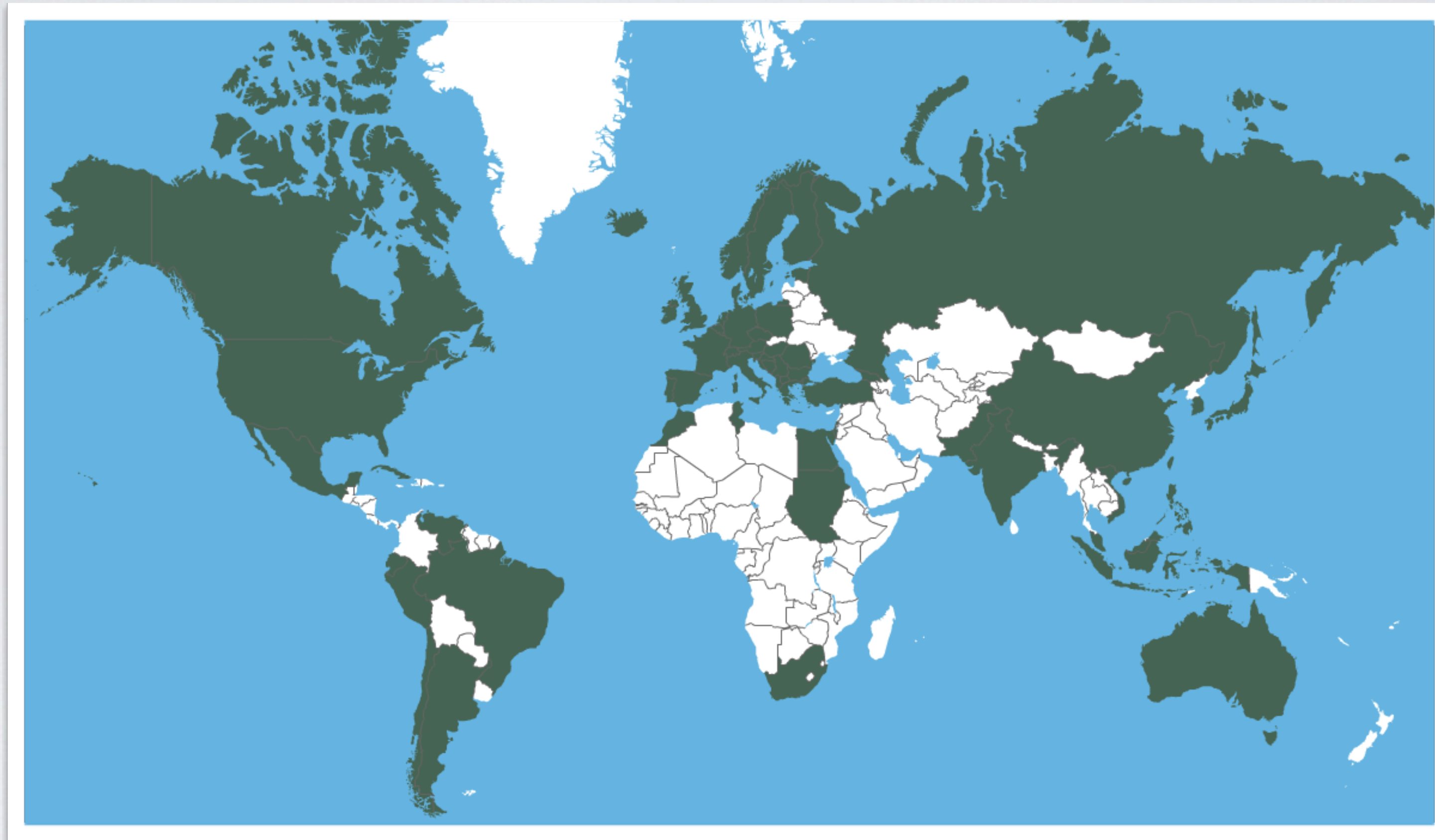


Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.  
Dans le cadre du CCRA, le produit est reconnu au niveau EAL4.  
Dans le cadre du SOG-IS, le produit est reconnu au niveau EAL4.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP



PICTURE TELLS 1000 WORDS



**world-wide**

# NEXT STEPS - IDEA

A combined software and hardware approach towards more trustworthy systems.

**H**ardware & **S**oftware **S**ecurity **P**latform - **HS<sup>2</sup>P**

# NEXT STEPS - IDEA

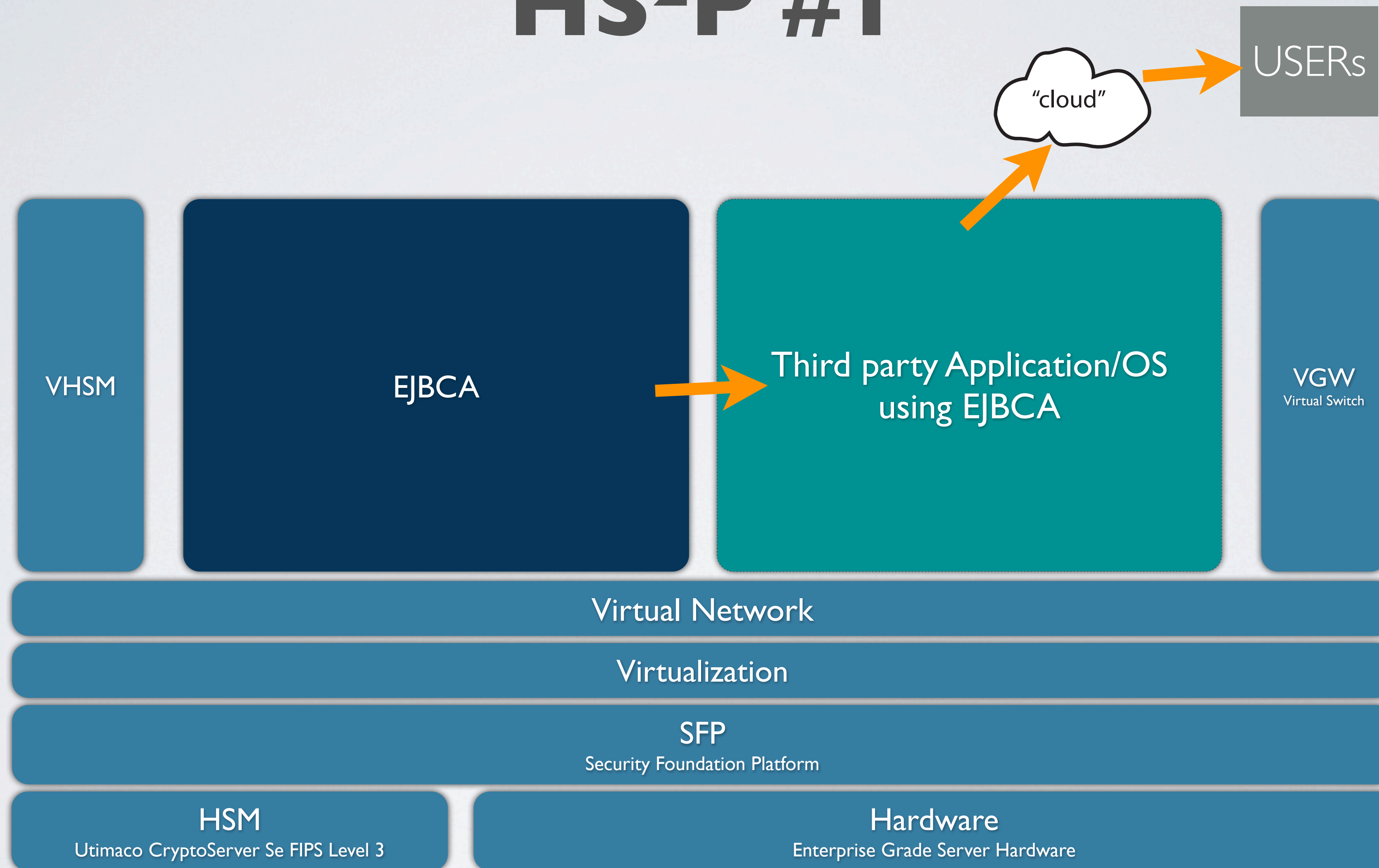
Bring security enhancements even closer to, and easier to deliver for “Real world” secure application vendors.

**H**ardware & **S**oftware **S**ecurity **P**latform - **HS<sup>2</sup>P**

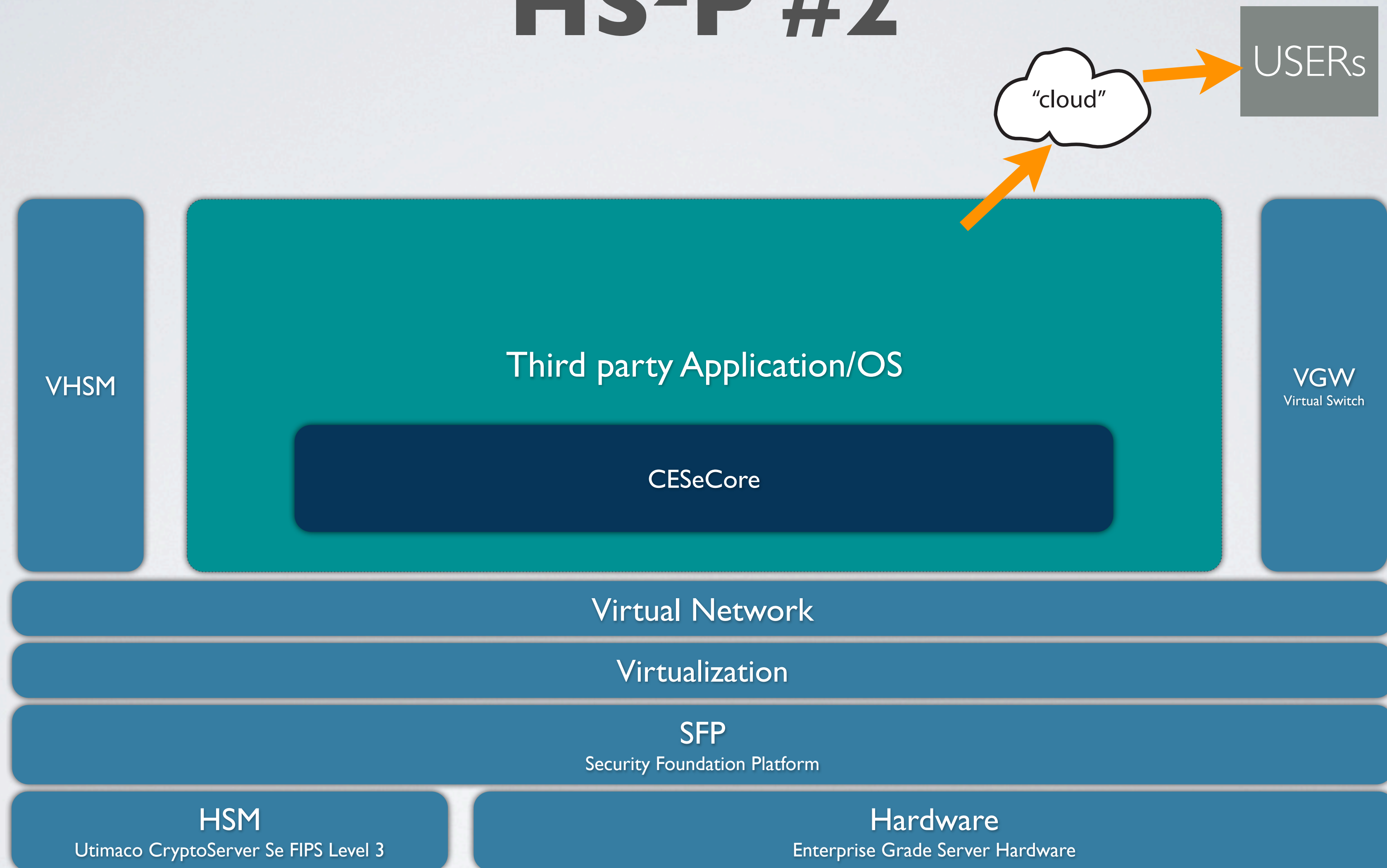
# CUSTOMER'S VALUE EXPERIENCE

- Deliver „Turn-Key” Secured Applications/Solutions, with Full Package:
  - Software - secured, certified, XX
  - Reliable hardware including HSMs
  - Best Practices and Services around secured applications/solutions
  - After sales support
- Customer
  - low internal effort; CAPEX vs OPEX
  - operational “immediately”
- Future Proofed Technology Stack (Tested Update Path)

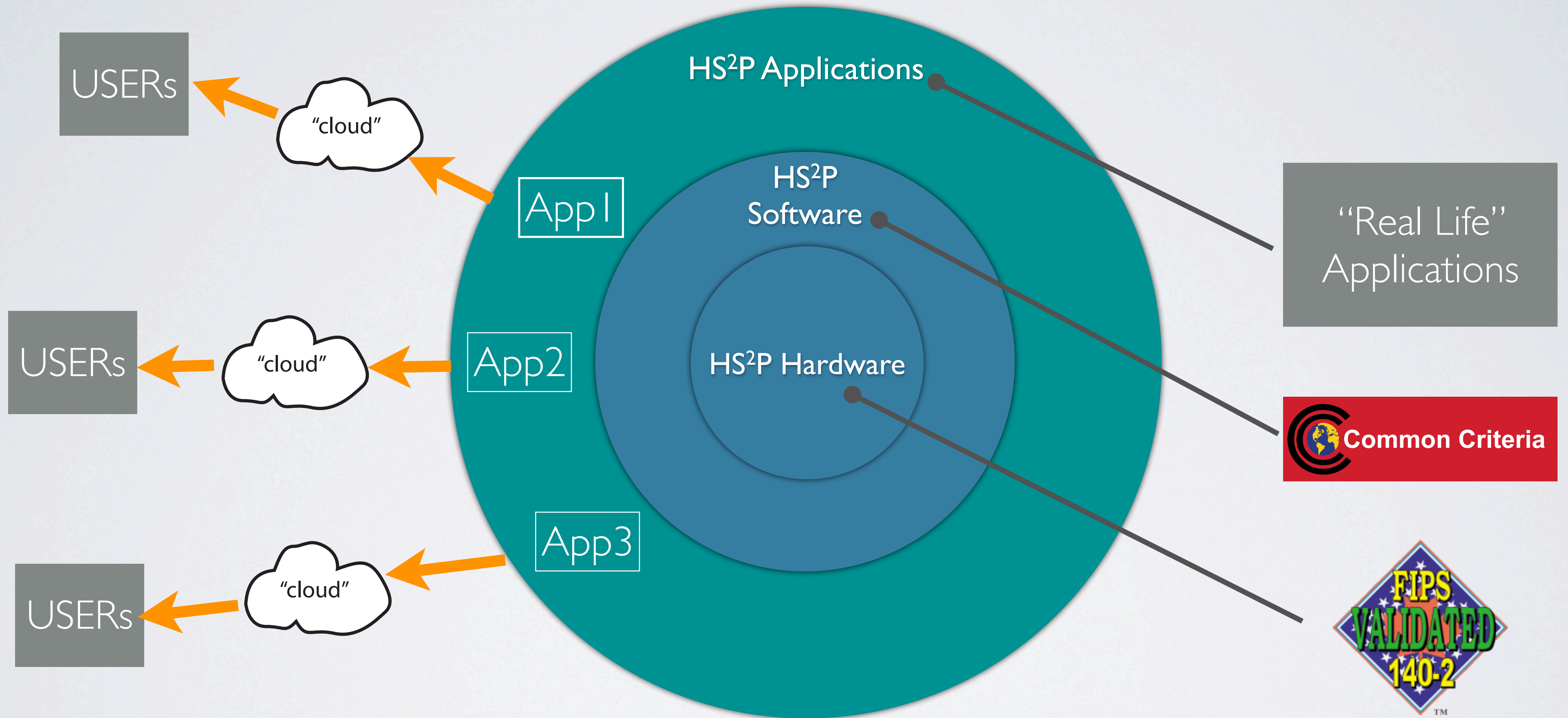
# HS<sup>2</sup>P #1



# HS<sup>2</sup>P #2



# HS<sup>2</sup>P ECOSYSTEM



# NEXT STEPS - CONCRETE

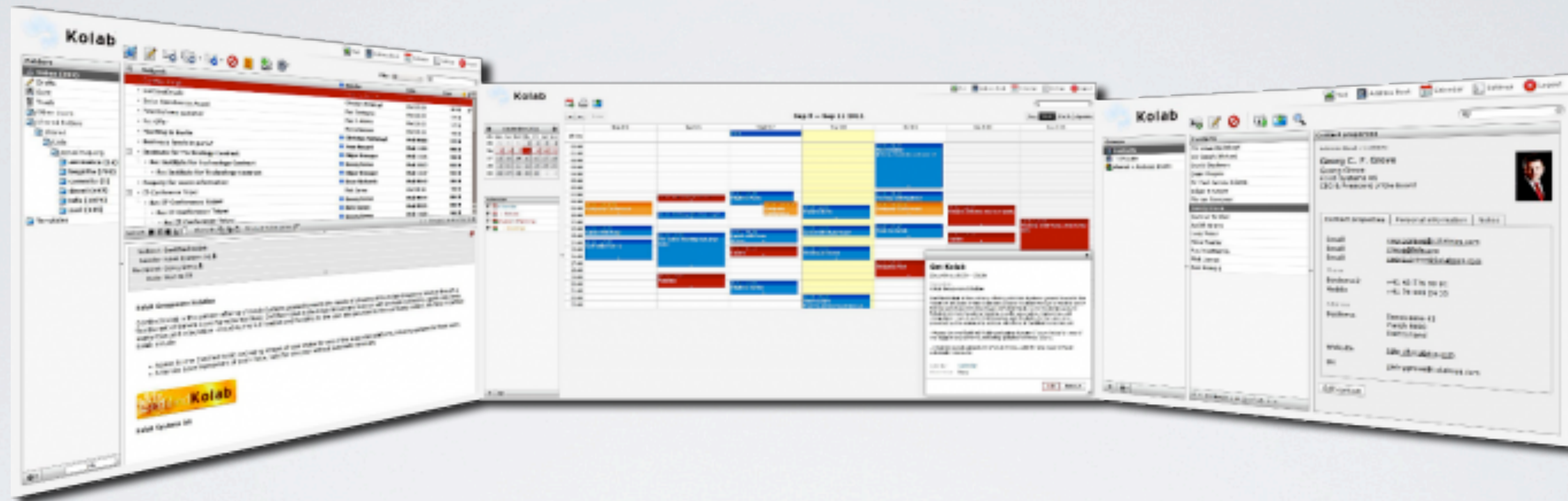
## **Secure Archival & eDiscovery**

Kolab Systems AG & PrimeKey Solutions AB

# SECURE ARCHIVAL & eDISCOVERY

- Concrete Business Drivers
  - USA, SEC rule 17A; the Sarbanes-Oxley Act
  - Switzerland, Geschäftsbücherverordnung (GeBüV)
  - EU, Data Protection Directive/Regulation
  - EU/ETSI, Long-Term Archiving (LTA), Long-Term Validity (LTV)
  - plenty other

# SECURE ARCHIVAL & eDISCOVERY



email, calendar,  
address books,  
tasks and files

associated  
transaction and  
modification  
records

stored with  
integrity  
protection,  
records cannot be  
altered or deleted

Records available  
upon requests,  
optional  
encrypted  
storage; indexable,  
restorable and  
searchable

# NEXT STEPS - CONCRETE

**PrimeKey (SME):**  
“integrity engine”,  
responsible for EU and  
commercial audit  
requirements

**Academia:**  
study collaboration  
methods, open  
development processes,  
“ORIOS”



**Kolab (SME):**  
data and user  
interfacing, responsible  
for archiving  
requirements

**Industry:**  
study the collaboration  
patterns, while  
addressing an important  
aspect of corporate  
infrastructure, and re-use  
of results

# NEXT STEPS - CONCRETE

**Other** (SME):  
we welcome your  
suggestions!

**PrimeKey** (SME):  
“integrity engine”,  
responsible for EU and  
commercial audit  
requirements

**Kolab** (SME):  
data and user  
interfacing, responsible  
for archiving  
requirements



**Academia:**  
study collaboration  
methods, open  
development processes,  
“ORIOS”

**Industry:**  
study the collaboration  
patterns, while  
addressing an important  
aspect of corporate  
infrastructure, and re-use  
of results

**Academia:**  
we welcome your  
suggestions!

**Other** (Industry):  
we welcome your  
suggestions!

# THANK YOU

[admin@primekey.se](mailto:admin@primekey.se)