ENTEGRITY Solutions

Token Interoperability and Portability Project

status report

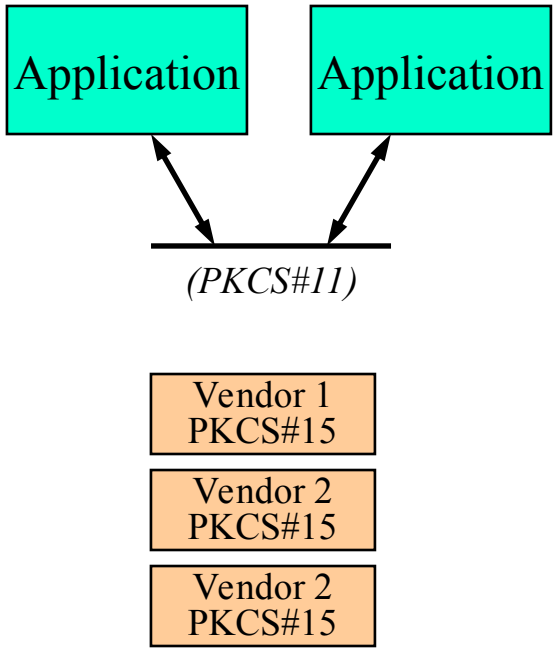
John Hughes

Montreal - 14 September 00

ENTEGRITY Solutions

Partial Solution

- PKCS#11 - with PKCS#15



Contain:

key pairs
trusted certs
user certs

But no good if no PKCS#11 or the Token needs PSE

Topics

- Scope
- Why the need?
- Status

Scope (abstract)

- The purpose of this white paper is to explore the problems with token interoperability and how the lack of token interoperability inhibits the deployment of PKI.In particular, the white paper should address:
  - a) The business requirements for Token Interoperability and Portability (hardware and virtual tokens)
  - b) The applicable environments (Windows, Java, etc), interface and driver technologies (CAPI, PKCS#11, PKCS#15, IETF sacred, OpenCard, etc)
  - c) The requirements for PKCS#11 conformance testing and potential groups to do this testing
  - d) The necessity to liase with the IETF and RSA/PKCS on the requirements for PKCS#11profiles, PKCS#15 and secure remote credentials
  - e) The requirement to produce a “Token Best Practises Guide” for CA, hardware token and client application vendors. This will detail what standards, profiles and testing they should meet to maximum token interoperability and portability

Why the need?

- Two main problems
  - PKCS#11
  - Token format
- Both of which are causing us “pain” - along with other suppliers and consumers

PKCS#11 example - Entegrity situation

- We have/are testing 13 PKCS#11devices from 6 suppliers working on either Wintel or Solaris platforms
- Total of 20 implementations
- Statistics:
  - only 6 implementations have passed our tests
  - we are waiting for patches from 4 of the suppliers
- More on testing - Thursday afternoon!

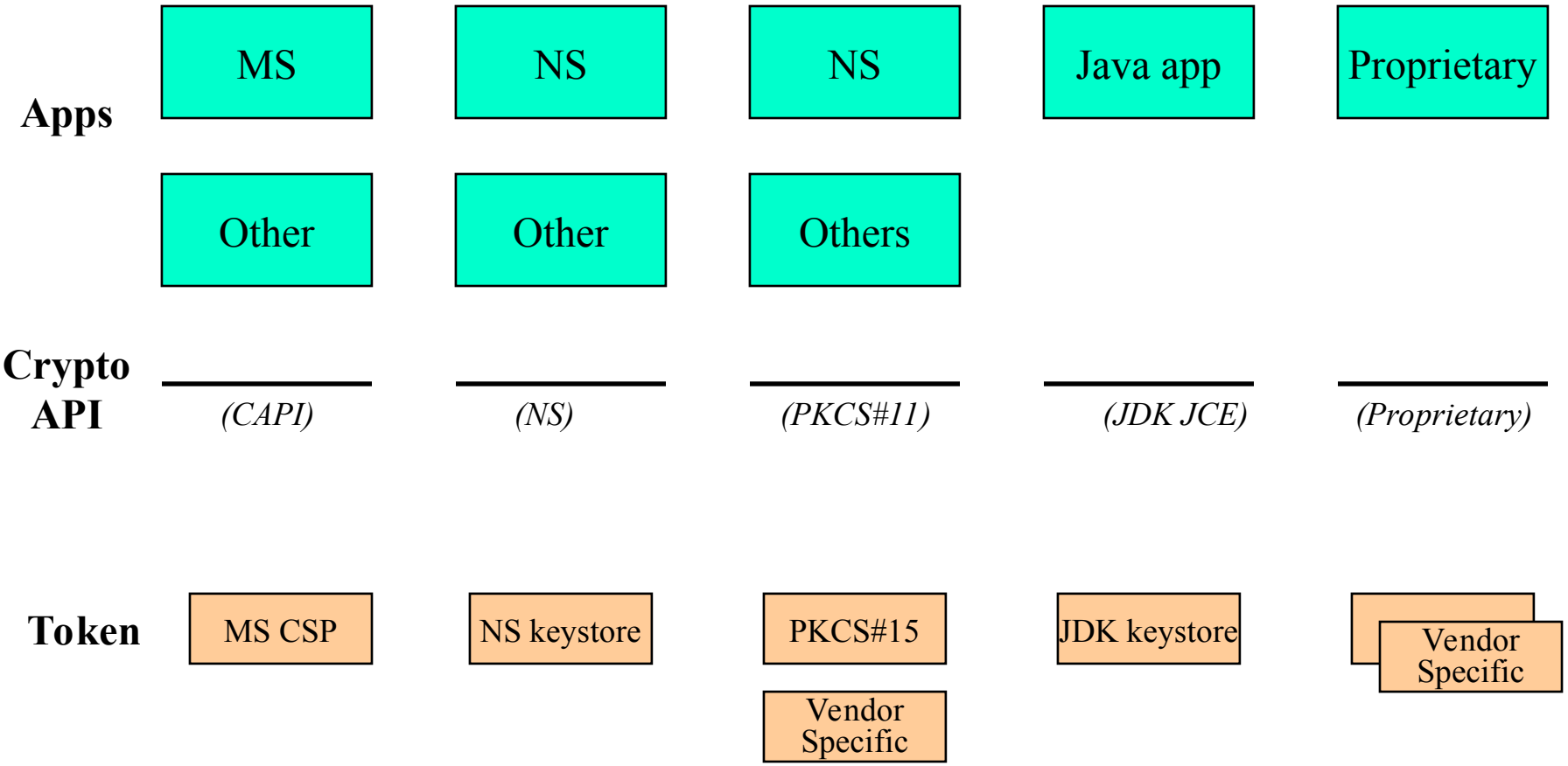
ENTEGRITY Solutions

Tokens

- As a minimum a Token usually is required to store
  - one or more private/public key pairs
  - one or more trusted public keys/certificates
- Optionally
  - user certificates
  - a PSE
- a wide range of types:
  - Entegrity SDP Token,Entrust Token,Baltimore Token etc etc
  - Java 1.2 keystore
  - PKCS#15 (hardware and software)
  - Netscape keystore
  - MS CSP
  - PKCS#12

ENTEGRITY Solutions

Complexity



ENTEGRITY Solutions

What customers want...

- A single key store/token
- applications from different vendors being able to access the same token

Why PSE?

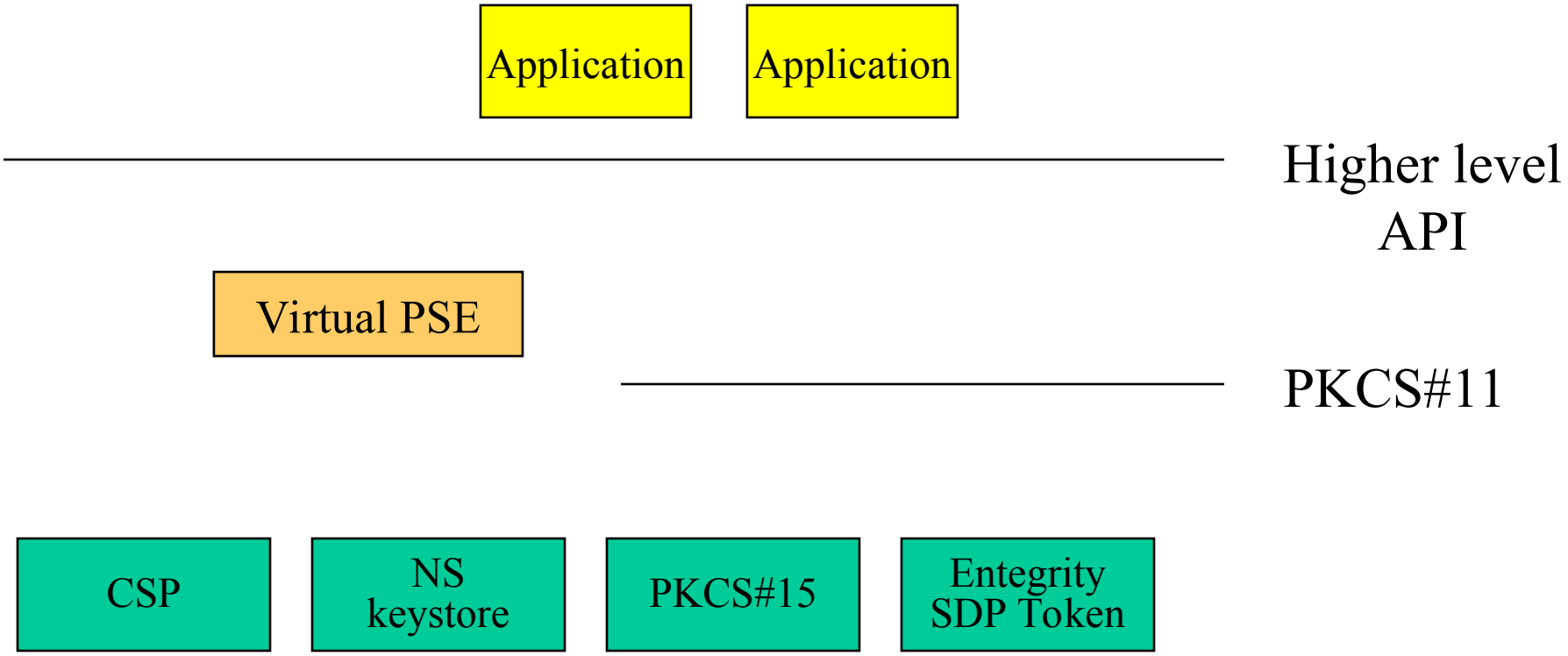
- If you:
  - have totally centralized management with no automatic key update/rollover etc
  - totally client key generation and the RA/CA enrollment process is via a browser (and no automatic key update/rollover)
- Then a PSE is not required

Why PSE - cont'd

- A PSE in the Token is a solution if you require "configuration" information in the Token - for example:
  - location and name of the parent CA
  - the protocol by which the communication with a CA is performed (e.g. PKCS#10/PKCS#7, PKIX(CMP) and transport)
  - key update period
  - PKIX CMP shared secret
  - CA policy e.g. min key size, token type
  - interdomain trust policy
- The PSE then permits a less intrusive PKI enrollment to take place (e.g. do not need to use browser to go to RA/CA site)

ENTEGRITY Solutions

Another Approach
Entegrity - Universal Token Support



Status

- White Paper:
  - Storyboard - issued on 3rd August on e-mail list
  - Request for Chapter Authors
  - Only 1 response - Laszlo Elteto (Rainbow Technologies)
  - Although many offers to review and “help”!!
  - Paper not very well progressed - lack of help + vacations
- PKCS#11
  - attending PKCS workshop
  - Discussions underway to look at having PKCS#11 compliance test for profiles (more on this Thursday)

ENTEGRITY Solutions

Storyboard

- CHAPTER 1 - Business requirements
  - 1.1 - outline purpose of the document
  - 1.2 - Introduce and state business needs for Token Interoperability and Portability.
- CHAPTER 2 - PKCS#11 and Device level APIs
  - 2.1 - Overview of PKCS#11
  - 2.2 - Why there are problems
  - 2.3 - Ongoing work with PKCS#11 conformance profiles
  - 2.4 - PKCS#11 testing - summary of what exists
  - 2.5 - detail and explain other relevant "stds"

Storyboard - cont'd

- CHAPTER 3 - Token Formats
  - 3.1 - overview of Token formats - e.g. PKCS#12, PKCS#15, NS token, MS/CSP Tokens, Java Key Stores, proprietary ones etc
  - 3.2 - detail minimum reqs of what should be in token -and refer off to Chapter 4 for remote credentials case
  - 3.2 - Provide scenarios of why this causes problems in user registration/enrolment - in both browser registration and more integrated cases
- CHAPTER 4 - Mobile Users and Remote Credentials
  - 4.1 - define requirements
  - 4.2 - summarise current state of IETF sacred work

ENTEGRITY Solutions

Storyboard - cont'd

- CHAPTER 5 - Recommendations
  - 5.1 - Detail "Token Best Practises Guide" for CA, hardware token and client application vendors. This will detail what standards, profiles and testing they should meet to maximum token interoperability and portability
  - 5.2 - Detail further work in the area required to be performed and any liaison work necessary

Conclusion

- New more volunteers - any?
- If none - then paper will take longer to produce