PKI interoperability issues for UK Government ... again

Richard Lampard
Richard.Lampard@cesg.gsi.gov.uk
... or,

The triumphant return of Richard Lampard!

Richard Lampard
Richard.Lampard@cesg.gsi.gov.uk
... or,

Oh dear, Lisa must really be scraping the barrel.

Richard Lampard
Richard.Lampard@cesg.gsi.gov.uk
Structure

1. Quick introduction
2. Why is interoperability crucial?
3. ALICE
4. Vendor interoperability trial
5. Summary
1. Quick introduction

- Communications-Electronics Security Group
  - a government agency
  - UK national Infosec authority
  - operates on a cost-recovery basis
  - aims to encourage adoption of PKI and related technologies by UK government, the armed forces and wider public sector

*Capitalising on the UK’s Sigint knowledge base, we will help to protect the nation’s security and safety, and deny foreign Sigint success*
2. Why is interoperability crucial?
2. Why is interoperability crucial?

• Encoding
  – DER versus BER
  – GeneralizedTime vs UTCTime
  – DN ordering
  – Base 64 vs ASN.1
  – PrintableString vs TeletextString
  – RFC 822 address included in DN
2. Why is interoperability crucial?

- Implementation problems
  - misinterpretations of standards, crass mistakes, incorrect assumptions, or “short cuts”
  - ASN.1 compiler bugs
  - arbitrary or machine limitations e.g. serial number length
  - inability to deal with incorrect or unexpected behaviour e.g. bad certification requests
2. Why is interoperability crucial?

- Directories (gulp!)
  - inability to use same Directory
  - schema clashes

- Proprietary private key token formats
2. Why is interoperability crucial?
2. Why is interoperability crucial?
3. ALICE

- Test level of interoperability provided by national implementations of international and NATO standards
- Hence, reduce risk to national procurements and developments
3. ALICE
3. **ALICE**

   STANAG 4406 interoperability
3. ALICE

STANAG 406 PCT with basic certificate exchange
3. ALICE

S/MIME and basic certificate exchange

STANAG 406

flags of Germany, France, UK, and USA

OCSG
3. ALICE

STANAG 4406
S/MIME and full PKI support
3. ALICE

SMTP S/MIME and full PKI support
3. ALICE
4. Vendor interoperability trial

- Previous interoperability work attracted some criticism
  - we didn’t always have most up to date version or based on beta code
  - not enough vendor involvement
  - test scenario did not present a level playing field
4. Vendor interoperability trial

- Invite vendors to participate
- Agree scenario
- Agree configuration
- Bake-off
- Assemble testbed
- Internet dry run
- Open to HMG users!
4. Vendor interoperability trial

• Why are we doing this?
  – give vendors the chance to prove their claims
  – … or enough rope to show otherwise
  – provides an up to date view of interoperability for products out of the box
  – shows CESG’s commitment to working with multiple vendors
  – shows CESG’s departmental customers the state of play

  – does anyone want to play?
5. Summary

• Lack of interoperability will still be a major problem for UK Government
• Key HMG efforts:
  – ALICE
  – vendor interoperability trial
  – and of course, participation in PKI Forum
5. Summary

PKI is done neither for personal acclaim (because the applications get all the glory), nor for financial gain (if you’re a civil servant).

Therefore, CESG PKI experts must be the purest form of security consultant.

Discuss.