SSR 2014: Security Standardisation Research
Tuesday, December 16, 2014, Session 2 - Standards Development

Standardization Transparency
- An Out of Body Experience

Phillip H. Griffin

Griffin Information Security Consulting

Telebiometric Information Security and Safety Management

Telebiometric System Heartbeat

Cryptographic Message Syntax (CMS)

Signcryption Support in CMS

Rubric — <u>Suggest Areas For New Standardization</u>

Broken Schema

The ICAO passport schema is based on invalid and deprecated IETF syntax

```
LDSSecurityObject {
   iso(1) identified-organization(3) icao(ccc) mrtd(1)
      security(1) ldsSecurityObject(1)
}

LDSSecurityObjectVersion ::= INTEGER { V0(0) }

AlgorithmIdentifier FROM PKIX1Explicit88

AlgorithmIdentifier ::= SEQUENCE {
   algorithm   OBJECT IDENTIFIER,
   parameters  ANY DEFINED BY algorithm OPTIONAL
}
```

Invalid

Deprecated, Invalid

Deprecated

The '88' stands for 1988 and deprecated, then withdrawn standards

Standards Defects

What's the harm in flawed security standards?

FRENCHELON

SORM

TEMPORA

U//FOUO) MYSTIC

NEEDED: More ways to report defects – propose new standards projects

There is a crack, a crack in everything

That's how the light gets in.

Cohen, *Anthem*

Thank You!

Comments?

phil@phillipgriffin.com +1 919 291 0019 Skype: phil.griffin