

# Automated Certificate Checks

David O'Callaghan

Trinity College Dublin · Grid-Ireland CA

17<sup>th</sup> EU Grid PMA · Berlin, Germany · September 2009





# GFD.125 AND POLICY COMPLIANCE TESTING

# Items to check for

- CA/Issuer certificate requirements
  - Name uniqueness (openssl x509 -subject)
  - RDN component ordering (openssl asn1parse -dump)
  - Version: must be v3
  - basicConstraints: critical? CA:FALSE? (openssl x509 -text)
  - keyUsage: only certSign, cRLSign?
  - CDP (if present) has http URL in URI attribute
  - Validity period: between 3 and 20 years, warn if <10
  - signatureAlgorithm: must be SHA-1
- CA/Issuer certificate other checks
  - Policy OIDs (should not be present)
  - eKU: check for weird attributes
  - Serial number: warn if 0, error if <0
- On update: Did serial number change?



# Items to check for in client cert

- EE cert requirements
  - Is the namespace unique? Does it match the meta-data? (openssl x509 -subject)
  - Is the RDN ordering correct (openssl asn1parse -dump)
  - basicConstraints: critical, CA:FALSE?
  - keyUsage: no serverAuth in personal cert?
  - eKU: does it match any netscape attributes?
  - aKI: contains only keyID, error if name or serial detected
  - nsCertType: matches eKU if present
  - CDP: must be included and must return DER CRL
- EE cert other checks
  - keyUsage: no nonRepudiation &c?
  - DC naming, matching registered WHOIS contacts



# Items to check for in meta-data

- `crl_url` is http
- `crl_url` yields a CRL issued by the CA
- `crl_url` can sustain 4Hz requests
- CRL validity is > 7 days (warn if >3days, manual if >31 days)
- email: address does not bounce
- alias is reasonable representation of CA name
- alias matches `[A-Za-z][-A-Za-z0-9]+`
- `ca_url` if present: gets CA cert, warn if missing
- url: leads to non-empty html or text page
- status: matches accreditation



# Automate checks

- CA / Issuer certificates
- End-entity certificates
- Meta-data

against

Requirements and Best Practices from GFD-C.125

# Certificate Checking Utility

The certificate checking utility should be

- Sys-admin friendly
- Use familiar scripting languages and libraries

**Perl & OpenSSL**

- **How to describe the tests?**
- **How to handle the certificates?**



# How to describe the tests?

- **Assertions & Comparisons**
- **Structure for a set of tests**

# A portable test format?

`<xml>` can be `<too>` verbose `</too></xml>`

`(s-exps are-nice (if (you-like (or 'lisp 'scheme))))`

but...

# Disadvantages

- Parser for XML/s-exps/JSON/...
- Still need to define a language for assertions and comparisons

# Quick & Dirty

- Use a standard Perl test framework

`Test::Harness` and `Test::More`

- Supports assertions and comparisons
- Get overall result for a test suite

Tied to Perl but does what we want.

# How to test the certificates?

Using Perl and OpenSSL

- OpenCA
- **Crypt::OpenSSL::X509**
- Net::SSLeay

# Crypt::OpenSSL::X509

by Dan Sully

- Basic access to subject, dates, pubkey, etc.
- No support for extensions, name components

# Extending Crypt::OpenSSL::X509

## Added support

- get extensions by OID or name
- get name components
- check object type
- handle common extensions of interest
- handle CRLs

# GFD-C.125 Test Suites

Test suites for

- Certification Authority certificates
- Host certificates
- Personal certificates
- Robot certificates



# Putting it all together

DEMO

# GFD-C.125 Test Coverage

**88** distinct provisions

**80** implementable as automated tests

others require checking multiple certs,  
online checks, or manual checks.

**61** tests implemented

**69%** coverage

**75%** of implementable provisions

# Compliance of IGTf CA certs

**22 out of 91 fully compliant**

**MUST**

**2 (from same CA) using MD5**

**SHOULD**

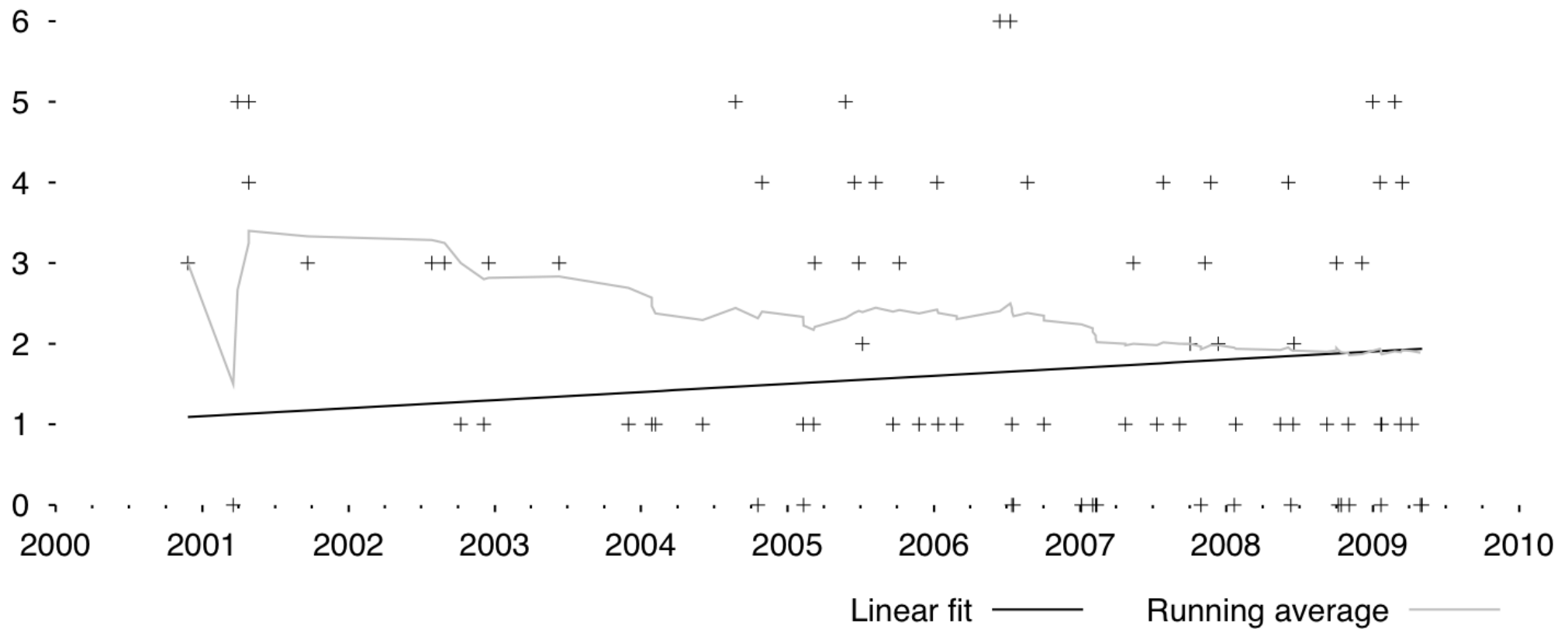
**39 have serial number = 0**

**32 include *nsCertType***

**22 have issues with the subject name**

**such as encoding or use of emailAddress**

# Compliance over Time



# Compliance over Time

**Very slight decrease in compliance over time**

= increase in failure

(I think)

Note that failures in the range 0 to 6 out of 61

# Other test suites

Initial port of IGTF-RAT test scripts

- CA certificates

MD5, RSA params, Debian keys

- CRLs

MD5

# Plans

- Extend coverage of GFD-C.125
- Tests for provisions in IGTf APs
- Implement on-line checks (e.g. is CRL in DER?)
- Highlight where a provision is unimplemented or requires a manual check in test output

# Ideas

- **Acceptance Matrix**

On-line state of CA cert compliance

- **Integration with other on-line tools**



# Links

<https://grid.ie/eugridpma/wiki/CheckCerts>

<http://github.com/davidoc/checkcerts>

[david.ocallaghan@cs.tcd.ie](mailto:david.ocallaghan@cs.tcd.ie)