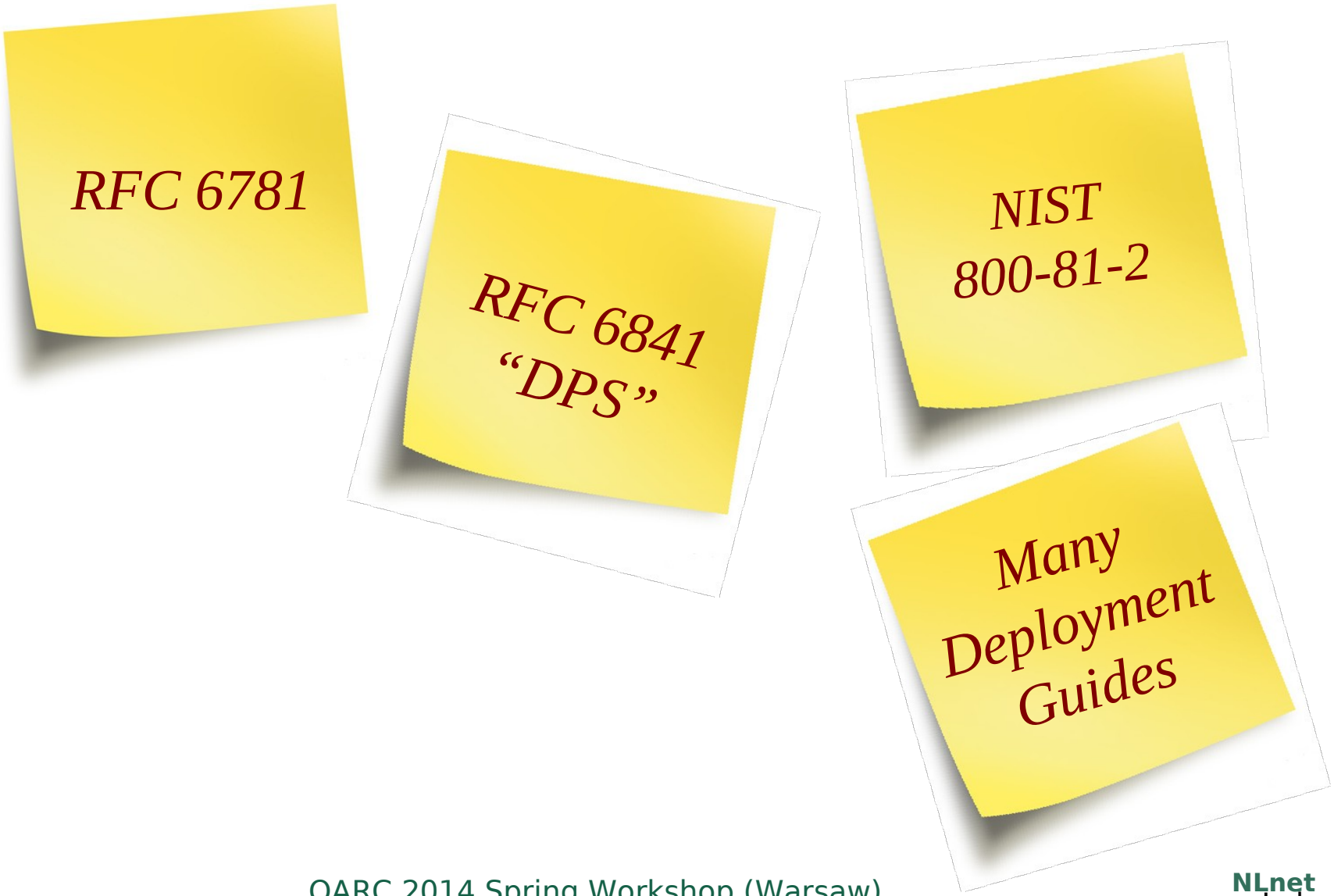
DNSSEC Audit Framework

W. Matthijs Mekking, Olaf M. Kolkman
matthijs@NLnetLabs.nl
olaf@NLnetLabs.nl

Background

- SWITCH wanted a second opinion
- NLnet Labs knows about DNSSEC
  - But we are no auditor

About DNSSEC



About auditing

Auditing DNSSEC

- A framework everyone can use
  - Creative Commons Attribution 4.0 International License 
- Targeted at TLD operators
  - But also useful for other DNSSEC operators

Auditing DNSSEC

- RFC 6841: DPS as a scope
- RFC 6781: Good practices
  - aka 4641bis
  - Additional practices from NIST document
- ISO 27008: loosely as methodology
- RFC 2119: MUST and SHOULD
  - Unless backed by managerial decision

Auditing DNSSEC

Objective

Control

Practice

Audit
* Interviews
* Examination
* Tests

For example

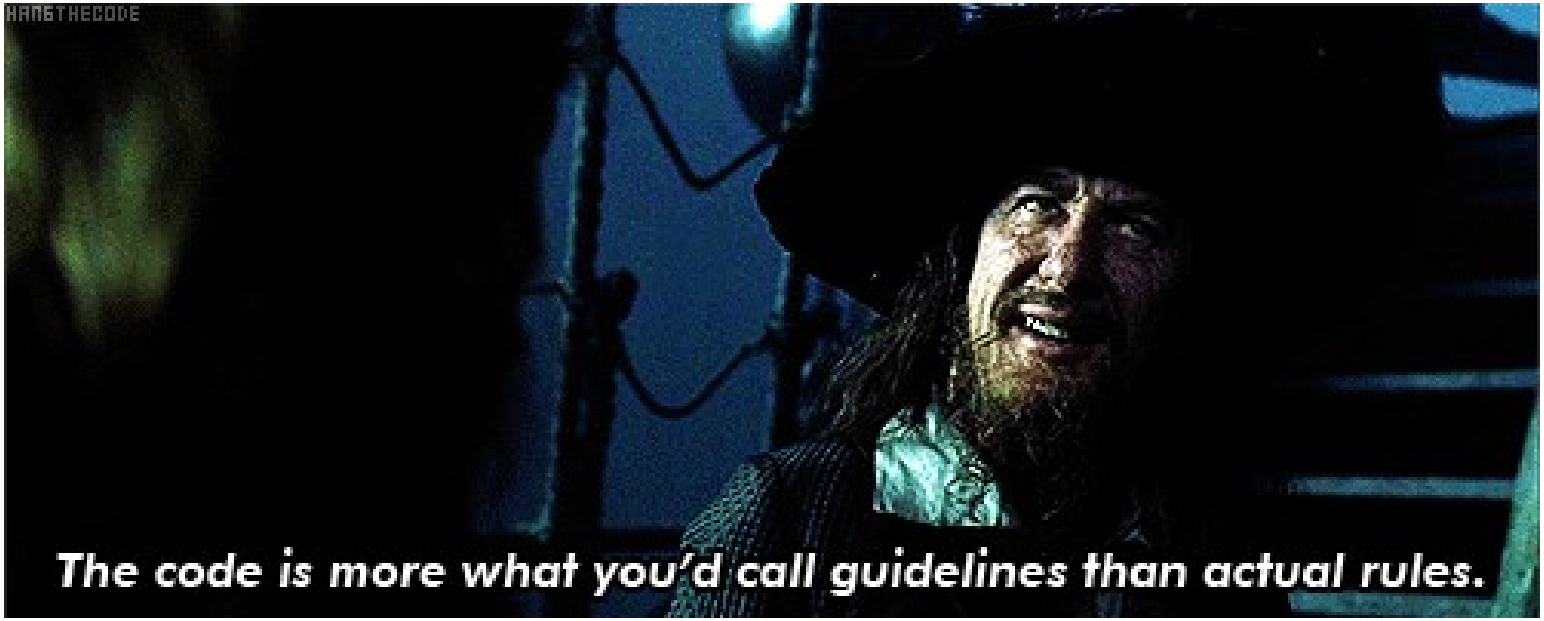
- DNSSEC Policy & Practice Statement
  - Objective: *Gain a shared understanding and transparency of choices and procedures for all stakeholders.*
  - Control: *Make the DP(S) publicly available.*
  - Practice: *SHOULD be easy accessible to the general public, SHOULD include all topics outlined in RFC 6841, …*
  - Audit: *Interview Security Officer, Examine publication mechanism, Examine DPS, …*

Framework outline

- 1. Introduction
- 2. Documentation
- 3. Facility and Management
- 4. Domain Name Registration System
- 5. Name Servers
- 6. Key Pair Handling
- 7. Technical Security Controls
- 8. Zone Signing
- 9. Zone Contents
- 10. Logging
- 11. Other Controls

More examples

- NSEC or NSEC3?
- Accepting DNSKEY or DS?
- Periodic or irregular key rollover?
  - No bad answers, if the underlying decision makes sense


HANGTHECODE
The code is more what you'd call guidelines than actual rules.

To summarize

- DNSSEC audit framework everybody can adapt and make use of 
- Work of

SWITCH **NLnet**Labs

- Feedback appreciated

http://www.nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf

http://www.nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf