# TLS Interoperability experiences

**Yngve N. Pettersen**
**Opera Software ASA**

draft-pettersen-tls-interop-experience-00.txt

# "Specification, meet Reality"

According to the SSL and TLS specifications various versions should be able to interoperate seamlessly.

In reality, some implementations does not work well with newer versions of TLS.

The problematic implementations are often used by high volume sites, e.g. online banking.

# Problem areas

Primary problem area centers around version number handling:

- Version negotiation
- Rollback protection
- Record protocol version handling

But TLS Extensions is also a problem, even for TLS 1.0 servers

# Possible reasons for problem?

- Misunderstandings of the text?
- Imprecise language in the text?
- Unavoidable complexity of the specification making it easy to miss details?
- Interoperability testing does not test limits?

# What can be done?

- Implementor's checklist?
- More examples about forward and backward compatibility?
- IETF hosted reference implementations?
- Stricter requirements to implementations about fallbacks?

# Way forward

## Document

- More examples, in particular from the server's side
- Information about how some problems emerged
- Other problems?

## After the document is finished

The problem, and possible solutions should be studied by the IESG