

Zope 3 C

Common Criteria Certification
of the Zope 3 security model

Europython Conference
Gothenburg, Sweden
June 2005

a project report by
Aroldo Souza-Leite
(Souza-Leite@mitcon.de)

Zope 3 C

(or ZSE : Zope Security Evaluation)

is a Zope community project started by

mitcon GmbH, Bonn, Germany

(main sponsor)

and

gocept GmbH, Halle, Germany

(project leader)

project wiki:

<http://www.zope.org/Wikis/DevSite/Projects/ComponentArchitecture/Zope3SecurityEvaluation>

Report topics

- Why Zope 3 deserves a security certificate
- The Common Criteria norm (ISO-15408)
- The task of certifying Zope 3
- The current state of the project
- Next steps
- Community support

The Zope 3 security model is a *thorough redesign* of the Zope 2 security model.

The Zope 3 security model is:

clear

solid

flexible

Clear implies documentable

and that there should be basically different types of security model documentations for basically different interest groups:

- Zope 3 beginners and advanced users
- Zope 3 developers
- executives and decision makers
- court appointed experts in lawsuits
- government agencies

thoroughly documentable

+

solid

implies

certifiable

by independent, government recognized
certification agencies.

Common Criteria (ISO-15408)

An international treaty establishing

- security documentation norms
- security testing norms
- further certification rules

for IT products

(<http://www.commoncriteriaportal.org>)

A very short list of the CC signatories (I)

USA:

- National Security Agency (NSA) and the
- National Information Assurance Partnership
(<http://niap.nist.gov/cc-scheme>)

A very short list of the CC signataries (II)

France:

Direction Centrale de la Sécurité des Systèmes
d'Information

(<http://www.ssi.gouv.fr/fr/confiance/methodologie.html>)

A very short list of the CC signataries (III)

Germany:

Bundesinstitut für Sicherheit in der
Informationstechnik

(<http://www.bsi.bund.de/cc>)

In which countries will the Zope 3 CC certificate be valid?

A security evaluation certificate issued by an auditor appointed by anyone of the signatory agencies is automatically valid in *all other signatory countries.*

The Job of certifying Zope 3

- Is taking place mainly in Germany. Auditor: Technischer Überwachungsverein (TÜV-IT)
- The core of the Zope 3 C team:
 - Christian Theune (project leader)
 - Steve Alexander (Zope 3 security system expert)
 - Jim Fulton (The Pope)
 - Aroldo Souza-Leite (contacts, information, PR)

Accomplishments up to now:

- initial negotiations with the audition agency and official admittance of Zope 3 to the certification process
- finding sponsors for the audition fees
- studying the ISO-Documentation rules
- first steps in authoring the ISO conform Zope 3 C documentation

Next steps

- finishing the ISO conform Zope 3 C documentation
- getting the documentation approved by the German auditor
- implementing a Zope 3 release with a typical security configuration (Zope 3 C)
- submitting the Zope 3 C release to the auditor

How the Zope community can support the project

- take notice of and co-edit the Zope 3 C documentation drafts in the project wiki
- participate in the Zope 3 C release implementation
- sponsor Zope 3 Security Model sprints and other organizational and management costs

Zope 3 C

clear

clever

certified