DFN CERT®

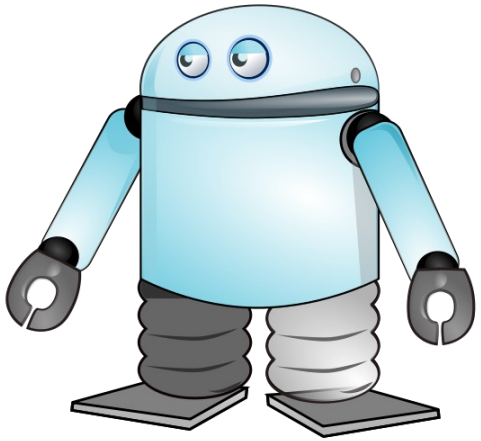
DFN Deutsches Forschungsnetz

Robot-Zertifikate

Jürgen Brauckmann
brauckmann@dfn-cert.de

Überblick

- Was sind Robot-Zertifikate?
- Wozu braucht man sie?
- Robot-Zertifikate im Detail



Was sind Robot-Zertifikate?

Was sind Robot-Zertifikate?

- „Fast normale” X.509 Grid-Zertifikate von einer akkreditierten Grid-CA
- **Client**-Zertifikate für automatische Prozesse
- Besondere Regelungen in der Policy
- Besondere Namen (DN):

  CN=Robot: Portal - RZ Ops - portal-ops@example.org
- Besondere Policy-Kennzeichnung (OID):

  1.2.840.113612.5.2.3.3.1

Wozu?

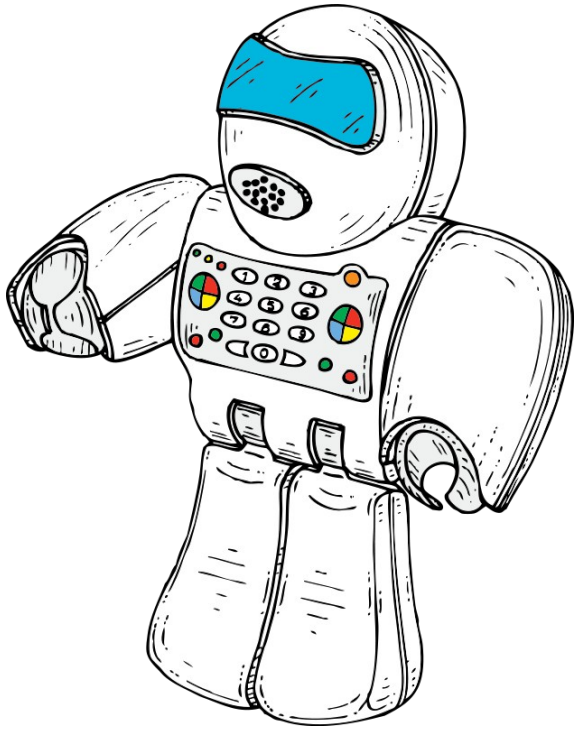
Wozu? (1)

- EUGridPMA: Anfangs nur Zertifikate für
  - Personen
  - Server/Services („Host-Zertifikate”)
- Problem: Automatische Clients/Prozesse, die Services nutzen, nicht vorgesehen
  - Beispiele: Monitoring-Anwendungen, Service-Portale
- Folge: Persönliche Nutzer- und Servicezertifikate wurden zweckentfremdet

Wozu? (2)

Lösung:

- Robot-Zertifikate!
- Kenntlichmachung von automatisierten Clients
- Vorgaben zum Handling



Robot-Zertifikate im Detail

Robot-Zertifikate (1)

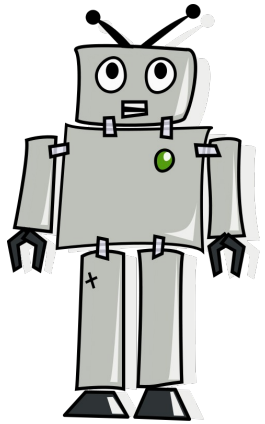
Historie:

- EUGridPMA:
  - Entwicklung von akzeptierten Regelungen für „Robots“, zunächst ausschließlich per Kryptotoken
  - EUGridPMA: „Guideline on Approved Robots”, 02/2010
- DFN: Policy-Änderung, um Robots zuzulassen (05/2010)

Robot-Zertifikate (2)

Verantwortlichkeit für ein Robot-Zertifikat:

- Immer mindestens eine natürliche Person!
- Gruppe auch OK, wenn durch die CA/RA auf mindestens eine nat. Person zurückführbar
- Personen werden im Robot-Zertifikat durch Namen und Mailadresse bezeichnet
- Gruppen durch Gruppen-Mailadressen
- Reaktionszeiten auf Anfragen:
  Ein Arbeitstag!



Robot-Zertifikate (3)

Namensbestandteile:

- Eindeutige Kennzeichnung durch „Robot:“ oder „Robot-“
- Beschreibung des Dienstes
- Entweder Name des Verantwortlichen (natürliche Person!) oder Mailadresse einer Gruppe

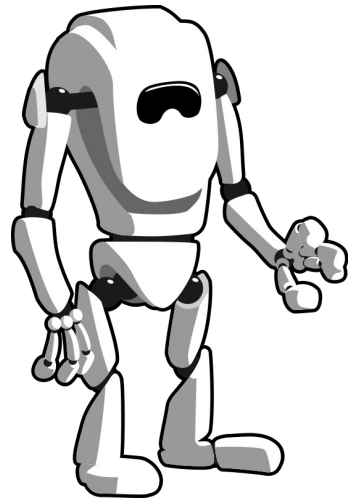
„CN=Robot: eSciencePortal - Dr. John E. Doe“

„CN=Robot: eSciencePortal - RZ Ops - portal@example.org“

Robot-Zertifikate (4)

Schutz des privaten Schlüssels:

- Entweder: HSM oder Kryptotoken
- Oder: Auf lokalem Filesystem eines Rechners, zu dem ausschließlich Robot-Betreiber Zugriff haben (Vorsicht, nicht so einfach, wie es aussieht!)
- Schlüssel nicht im Klartext
- „Sicherer“ Rechner
- Aktives Monitoring
- Physikalische Sicherheit („secured room“)



Robot-Zertifikate (5)

- Ressourcen können nach Zertifikatstyp differenzieren:
  - Personen-Zertifikate notwendig oder
  - Nutzung durch Robot-Zertifikate möglich
- Akzeptierter Zertifikatstyp könnte im GRRS vermerkt werden

Robot-Zertifikate (6)

Robot-Zertifikate in der EUGridPMA:

- CERN
- DutchGrid (Krypto-Token)
- GridGermany
- INFN-CA (Krypto-Token)
- UK eSciences CAs (Krypto-Token)

Zusammenfassung

- Robot-Zertifikate zur Verwendung in automatisierten Clients
- Zwei Ziele:
  - Kenntlichmachung von automatisierten Clients im Grid
  - Vorgaben zum sicheren Handling
- Technisch „nichts Besonderes“: Policy-OID, Schutz des Schlüssels
- Spezielle organisatorische Regelungen: Namensregelungen, Verantwortlichkeiten

pki@dfn.de
https://www.pki.dfn.de