# TCS
# lesson learned

Jana Kejvalová, Jan Chvojka
CESNET

# CESNET NREN situation

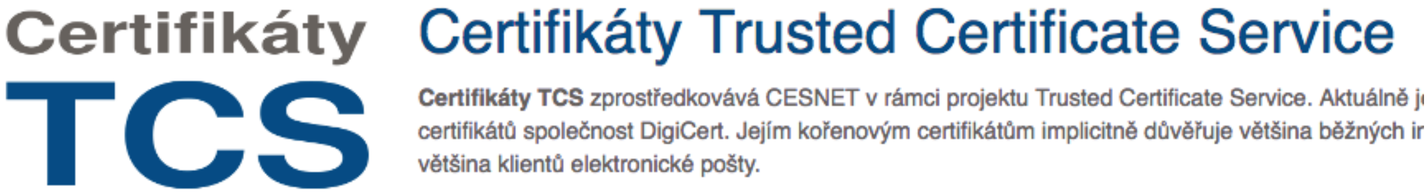
Organizations under CESNET NREN can get three types of certificates: with organization’s name containing diacritics, without diacritics and with English version

Example:

- CESNET, zájmové sdružení právnických osob
- CESNET, zajmove sdruzeni pravnickych osob
- CESNET

# CESNET NREN situation

CESNET is running own TCS portal. It communicates with DigiCert via DigiCert API. It offers Czech UI and possibility of additional CSR approval. It hides existence of non-grid personal certificates (as they don’t have unstructuredName). All information is stored in CESNET’s LDAP.



Certifikáty
TCS

Certifikáty Trusted Certificate Service

**Certifikáty TCS** zprostředkovává CESNET v rámci projektu Trusted Certificate Service. Aktuálně j
certifikátů společnost DigiCert. Jejím kořenovým certifikátům implicitně důvěřuje většina běžných ir
většina klientů elektronické pošty.

# CESNET NREN situation

Dun & Bradstreet – we don't have one

ARES (register of economic subjects) – no phones provided

Yellow pages – obsolete or wrong information, staff on these numbers sometime don't speak english (even at universities!)

# CESNET NREN situation

Some administrators are not enough technically skilled.

DigiCert don't want to exactly describe validation process.

So CESNET is not able to provide proper detailed documentation.

# Expectations

DigiCert would warn administrators when domain / organization / administrator validation is going to expire.

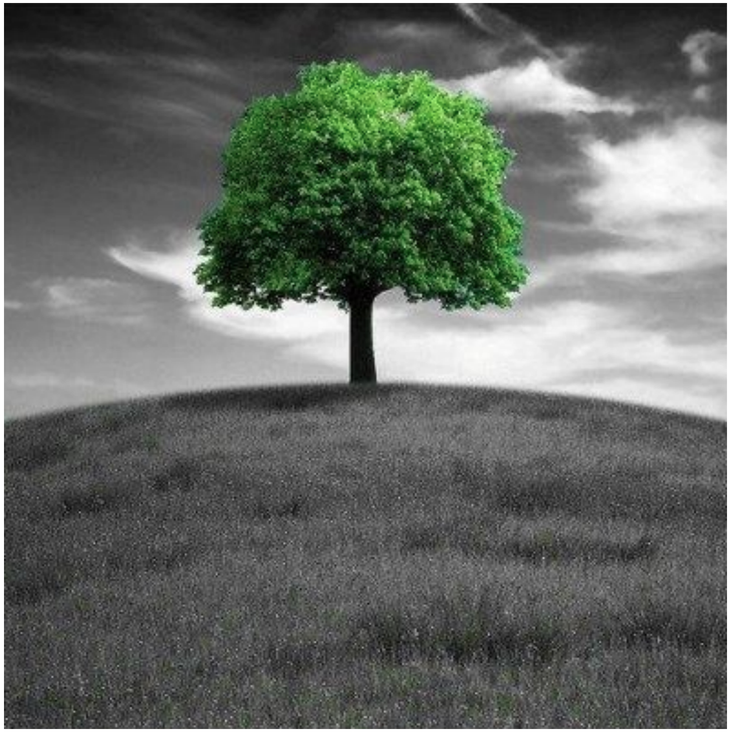
DigiCert wouldn't change name of any organization.

...

# Reality

Dear friend, all theory is gray,
and green the golden tree of life.

J. W. von Goethe: Faust



# Golden tree of life

**case #1 - incompetent operator**

Telephone operator doesn't speak any foreign languages, hearing foreign language causes immediate hang up.

**case #2 - wrong information in Yellow pages**

Telephone number in yellow pages leads to dormitory. TCS administrator at organization doesn't have will / power to change it.

# Golden tree of life

During validation process DigiCert sometimes changes organization’s name.

It is…

…pretty punk sometimes.

# Golden tree of life

## Adding whitespace:

Original: O=BRAILCOM,o.p.s
Changed to: O=BRAILCOM, o.p.s.

## Deleting commas:

Original: O=Gymnázium Matyáše Lercha, Brno, Žižkova 55, příspěvková organizace
Changed to: O=Gymnázium Matyáše Lercha, Brno Žižkova 55 příspěvková organizace

## Shortcut + adding accented character:

Original: O=Vyzkumny ustav geodeticky, topograficky a kartograficky, v. v. i.
Changed to: O=VÚGTK, v.v.i.

# Golden tree of life

## Getting rid of diacritics:

Original: O=Vyšší odborná škola informačních služeb, Praha 4, Pacovská 350

Changed to: O=Vyssi odborna skola informacnich sluzeb, Praha 4, Pacovska 350

## Upper/lower case (Pilsen is a town):

Original: O=Center for School Services Pilsen

Changed to: O=Center for School Services pilsen

## WTF?! name change

Original: O=General High School

Changed to: O=Cheb Grammar School

# Solutions

**Wrong phone number, incompetent administrators**

Communicate, communicate, communicate. When all above fails, we try to communicate instead.

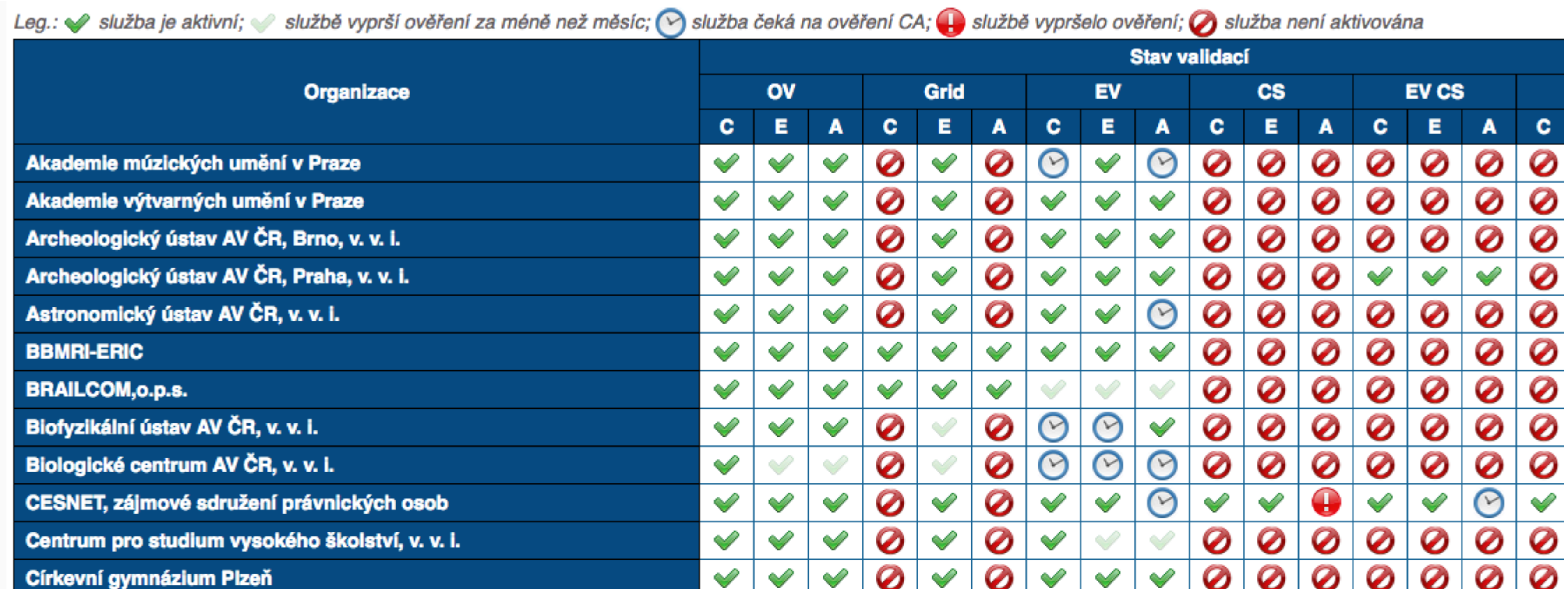
**Expired validations**

CESNET developed system for automatic validation checking and asking DigiCert to validate.

**Names changes**

CESNET developed system for tracking changes at DigiCert side.

# Validations checking



*Leg.: ✔ služba je aktivní; ✓ službě vyprší ověření za méně než měsíc; 🕒 služba čeká na ověření CA; ❗ službě vypršelo ověření; 🚫 služba není aktivována*

| Organizace | Stav validací | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OV | | | Grid | | | EV | | | CS | | | EV CS | | | |
| | C | E | A | C | E | A | C | E | A | C | E | A | C | E | A | C |
| Akademie múzických umění v Praze | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | 🕒 | ✔ | 🕒 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| Akademie výtvarných umění v Praze | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✔ | ✔ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| Archeologický ústav AV ČR, Brno, v. v. i. | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✔ | ✔ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| Archeologický ústav AV ČR, Praha, v. v. i. | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✔ | ✔ | 🚫 | 🚫 | 🚫 | ✔ | ✔ | ✔ | 🚫 |
| Astronomický ústav AV ČR, v. v. i. | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✔ | 🕒 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| BBMRI-ERIC | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| BRAILCOM,o.p.s. | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✓ | ✓ | ✓ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| Biofyzikální ústav AV ČR, v. v. i. | ✔ | ✔ | ✔ | 🚫 | ✓ | 🚫 | 🕒 | 🕒 | ✔ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| Biologické centrum AV ČR, v. v. i. | ✔ | ✓ | ✓ | 🚫 | ✓ | 🚫 | 🕒 | 🕒 | 🕒 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| CESNET, zájmové sdružení právnických osob | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✔ | 🕒 | ✔ | ✔ | ❗ | ✔ | ✔ | 🕒 | ✔ |
| Centrum pro studium vysokého školství, v. v. i. | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✓ | ✓ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |
| Církevní gymnázium Plzeň | ✔ | ✔ | ✔ | 🚫 | ✔ | 🚫 | ✔ | ✔ | ✔ | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 | 🚫 |

# CESNET’s TCS ecosystem

- System for registering new organizations
- System for issuing certificates
- System for domain/organization/administrator validation checking
- System for name changes checking
- System for certificate ongoing expiration checking

**...isn’t it too much?**

# Result

**Yes, it is!**

Programming / running these systems
is too programmer / operator consuming.
Also time to time DigiCert API changes
and we must react to these changes.

CESNET’s TCS portal is mission critical,
many organizations rely on us.

Support for generating CSR in browsers
is constantly decreasing.

# Result

We highly **discourage** other NRENs to run their own portal, although it would be helpful for us to share experience.

It would be awesome in the future to have Czech UI on standard portal (CESNET can help with translation).

We resigned to have three organization's names for the future versions.

# (our) Questions?

**We would be happy to hear from other NRENs:**

Is nonexistence of your native language UI problem for your organizations?

What would you do when the browser CSR generation support is gone tomorrow?

Are you using diacritics in organization names (O=…)?
If so, what about grid certificates?

# Time for your questions!

Further comments / questions please send to
ca@cesnet.cz

# Thank you!