SWITCHpk News

Andres Aeschlimann
andres.Aeschlimann@switch.ch

Bern, 14.3.2018
SWITCHpki

Customer tailored SSL-certificates
SWITCHpki delivers customer tailored SSL-certificates for servers and users

Customers
- Universities
- University related organizations

Services
- OV-/EV certificates
- Purchase options retail or bulk (500+)

Your benefits
- Rapid ordering process
- Customer tailored certificates
Situation in 2016

We are grateful for the information in this presentation provided by our partner WiseKey/QuoVadis
Situation in 2017

- Comodo: 28%
- GoDaddy: 0%
- GlobalSign: 18%
- DigiCert: 13%
- Let's Encrypt: 6%
- Entrust: 0%
- Others: 5%

© 2018 SWITCH | 4
Let’s Encrypt

• Increase in market share from 4 to 28% in one year
• DevOps minded: Automation and scalability in everything they do
• DV means: Keep encryption, while leaving identity
• Certificates have a lifetime of 90 days
• Everything newly developed
## More statistics

<table>
<thead>
<tr>
<th></th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Certs</td>
<td>5.2 Mio</td>
<td>5.7 Mio</td>
</tr>
<tr>
<td>ECC Certs</td>
<td>24’000</td>
<td>370’000</td>
</tr>
<tr>
<td>Short lived (&lt;2 months)</td>
<td>480’000</td>
<td>1.2 Mio</td>
</tr>
<tr>
<td>EV Certs</td>
<td>~ 5%</td>
<td>shrinking</td>
</tr>
</tbody>
</table>
Shorter validity of certificates

• Once upon a time you could have certificates that were valid for 5 years
• Validity has now been cut down to 825 days (approx. 2 years and 3 months) by the CA Browser Forum (*pushed by the browser companies*)
• Validity of only one year is foreseeable
• Let’s Encrypt is already at 90 days
More facts and trends

• Automatic Certificate Management Environment (ACME) becomes an IETF Specification:
• Certificate Transparency has now an RFC:
• Next step: all new trusted SSL certificates must be logged by CA’s by April 2018.
  https://casecurity.org/2017/05/03/certificate-transparency-deadline-moved-to-april-2018/
• DevOps (Let’s Encrypt) predominant
• Squeeze on small providers
• Google is setting up their own trust services
• So does Amazon
The role of SWITCH

1. Closely watch the market
2. Share information and report back to the Community
3. Listen to you
4. Find appropriate solutions for the Academic Community
5. Go to step 1
## Links

[CT-Observatory](https://www.ct-observatory.org/)

<table>
<thead>
<tr>
<th>Common Name</th>
<th>Issued by</th>
<th>Not Before</th>
<th>status</th>
<th>Not After</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.switch.ch">www.switch.ch</a></td>
<td>QuoVadis EV SSL ICA G1</td>
<td>2018-01-16 12:02:45</td>
<td>active</td>
<td>2020-01-16 12:02:00</td>
</tr>
<tr>
<td><a href="http://www.switch.ch">www.switch.ch</a></td>
<td>QuoVadis EV SSL ICA G1</td>
<td>2017-10-19 09:03:51</td>
<td>active</td>
<td>2019-10-19 09:13:00</td>
</tr>
<tr>
<td><a href="http://www.switch.ch">www.switch.ch</a></td>
<td>QuoVadis EV SSL ICA G1</td>
<td>2017-02-09 12:46:44</td>
<td>active</td>
<td>2019-02-09 12:56:00</td>
</tr>
<tr>
<td><a href="http://www.switch.ch">www.switch.ch</a></td>
<td>QuoVadis EV SSL ICA G1</td>
<td>2016-04-12 08:30:02</td>
<td>active</td>
<td>2018-04-12 08:40:00</td>
</tr>
<tr>
<td><a href="http://www.switch.ch">www.switch.ch</a></td>
<td>QuoVadis Global SSL ICA</td>
<td>2010-08-05 07:48:10</td>
<td>expired</td>
<td>2012-08-04 07:48:10</td>
</tr>
</tbody>
</table>
Consequence of CT

https://crt.sh/?zlint=1+week&dir=^&sort=7
Links

https://cabforum.org/baseline-requirements-documents/