Karlsruher Institut für Technologie

International Grid Trust Federation
AP | EU | TAG

IGTF Communication Test 2015 Report

Ursula Epting

STEINBUCH CENTRE FOR COMPUTING - SCC

Report overview

Two parts

Part 1 - results of communication challenge

Part 2 - results of additional questions regarding usage of sha1/2

Ursula.Epting@kit.edu

Part 1 Motivation

The intention of the test was to check whether the registered email addresses of accredited IGTF-CA's are correct and how good communication works.

➡ correct email addresses are the basis for all communication

➡ effective communication is essential in an infrastructure providing elementary security, like the IGTF PKI

Why should we care?

In case of a security incident, where a certificate is compromised, it is very important that a CA quickly processes revocation requests (means: revoke a certificate and issue a new crl)

Part 1 Description and execution

The test started with the announcement that a communication test will be executed within the next 3 weeks. This information went to all accredited CA's, included in the IGTF-Release 1.69.

These CA's then received an email and have been requested to answer **within one business day**. If no replies arrived reminders were sent to that CA's. Additionally they were asked two questions which could be answered within one week. (Part two of this talk)

The number of CA's in the IGTF-release at the time of testing was 96.

Notice: 'A CA' refers again to one CA-certificate. If there is a hierarchical structure with e.g. root-, server-, user-CA this will count as three CA's while in fact it is only one CA-structure.

Part 1 Timeline of the test/challenge

6th November, Announcement of the test

25th November, 12.00 h, Start of the test

26th November, 12.05 h, Reminder for not replying CA's

27th November, 13.00 h, 2nd Reminder

28th November, End of the test

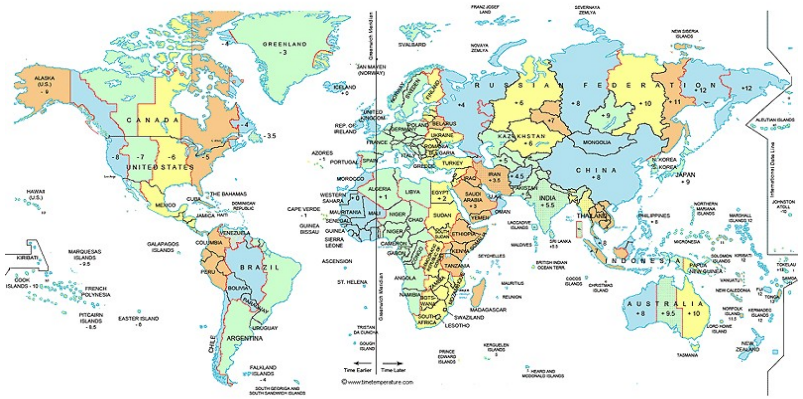
Notice 1: The specified test times refer to time zone UTC/GMT +2, CEST +1

Notice 2: no reminders were sent for the two additional questions

Part 1 Time measurement

As the test victims are spread all over the world and therefore live in different time zones, the target response time 'within one business day' was interpreted as 24 h refering to the location of the test sender.

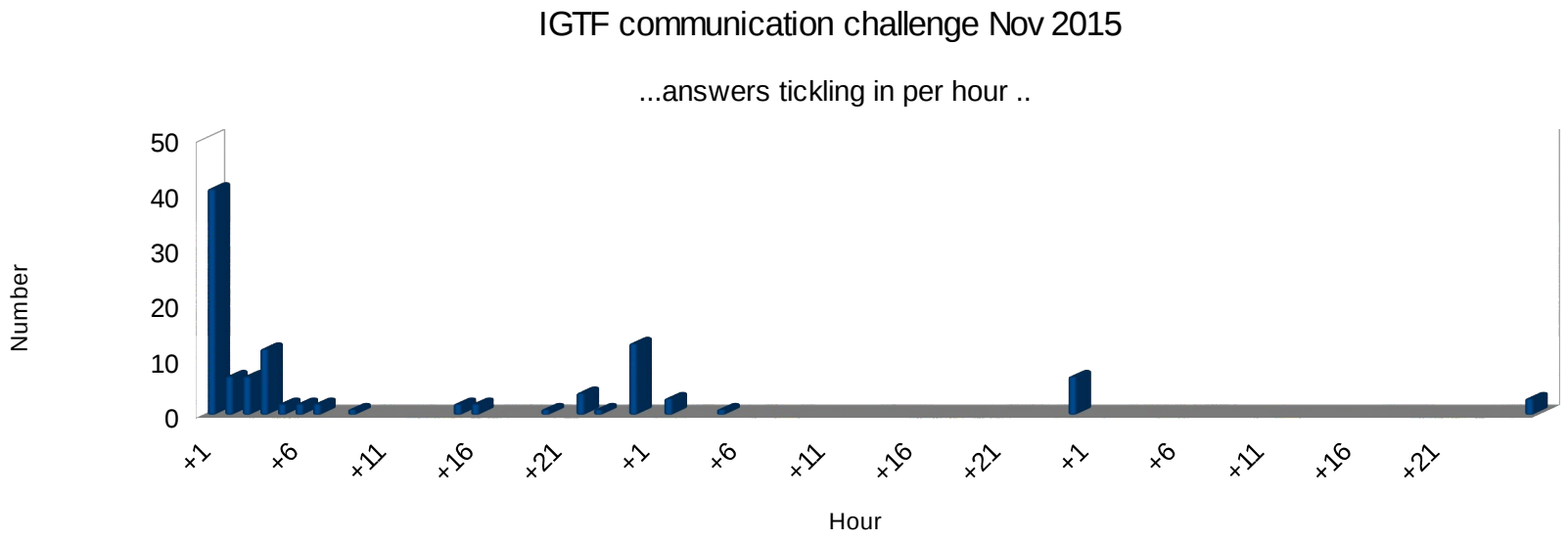
Response times were also measured in this sense. All emails received by the test sender within 1 hour after the start of the test, count for 'CA replied within 1 hour' regardless of the timezone of the CA.



Ursula.Epting@kit.edu

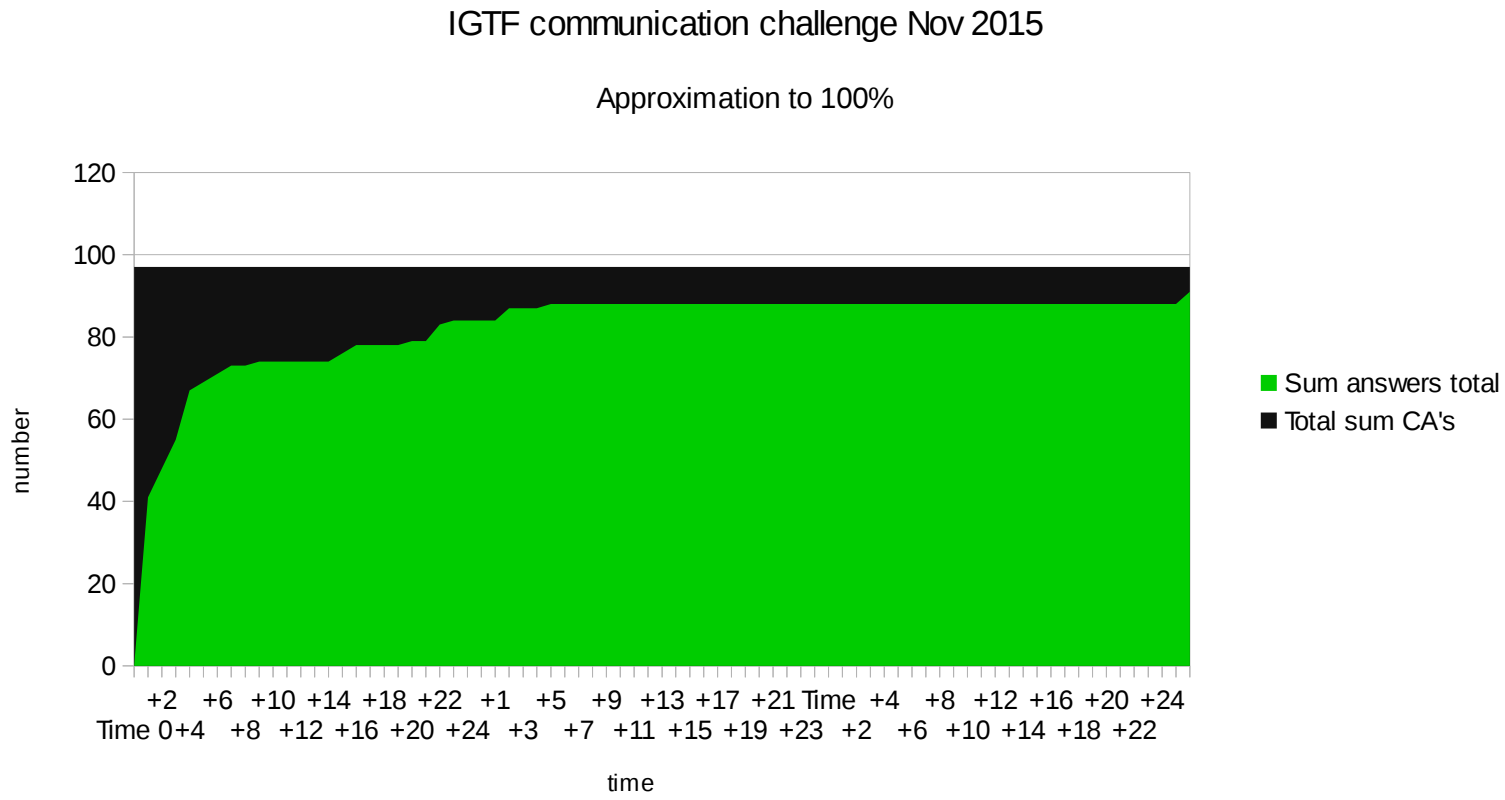
Part 1 Results – detailed view (1)

42 % of the CA's have replied within the first hour (last time 30%), which shows that there was again a very high motivation to contribute to a successful test result!



Ursula.Epting@kit.edu
Steinbuch Centre for Computing

Part 1 Results - detailed view (2)

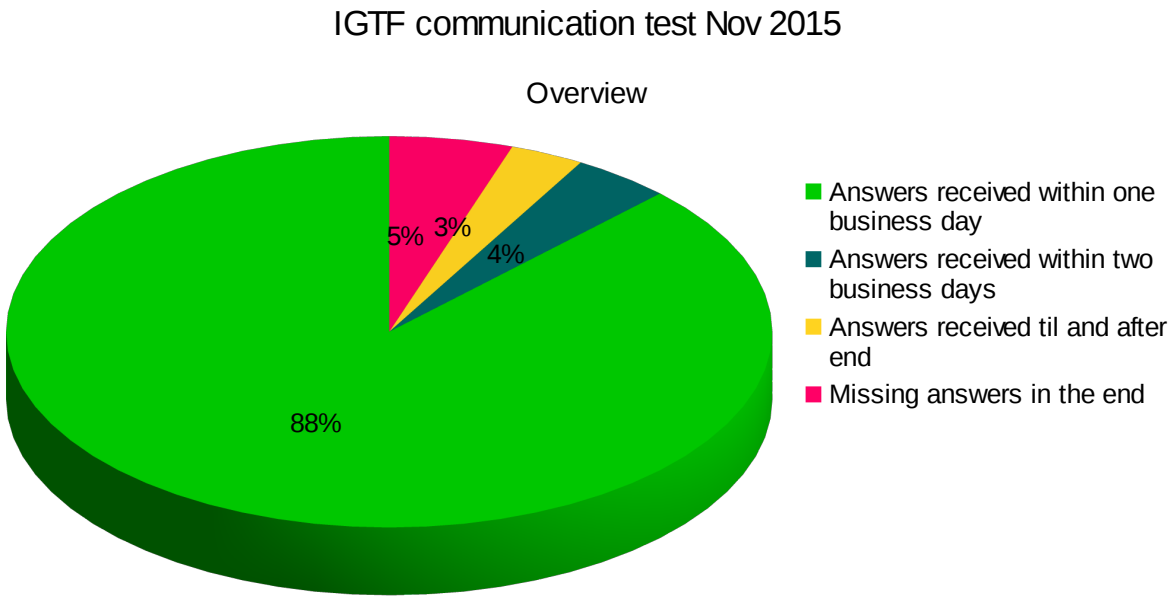


So answers from 100 % of all CA's has not been reached, but 88 % (hard) or 92 % (soft) or 95 % (very soft) have been responsive.

Ursula.Epting@kit.edu
Steinbuch Centre for Computing

Part 1 Results complete view

The big majority of 88 % replied within 24 hours/one business day.

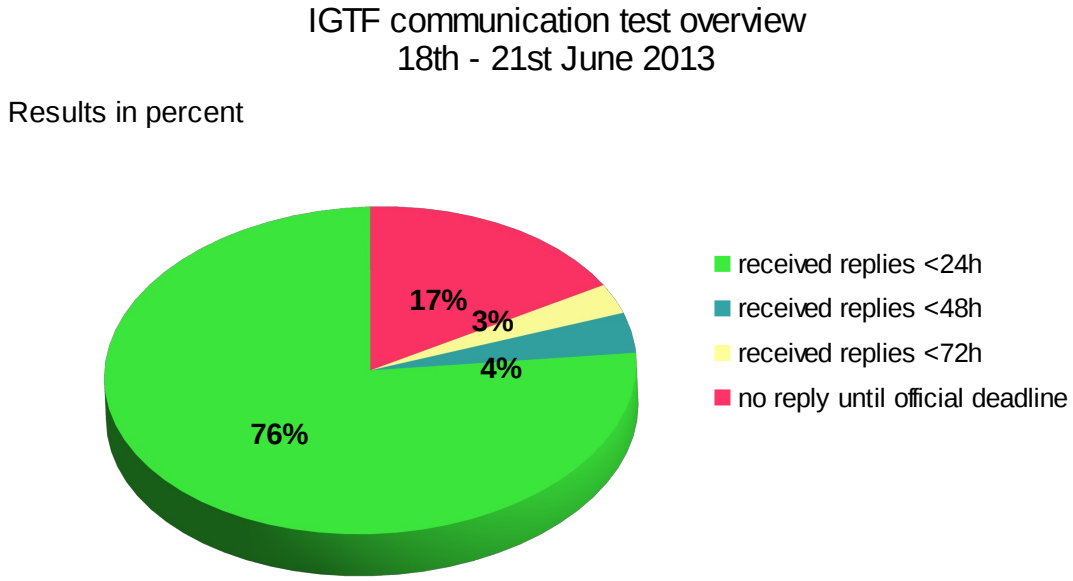


Additionally 4% replied within 48 hours and 3 % replied later
5 % did not reply at all.

Notice: automatic replies of e.g. ticket systems were not counted

Part 1 Comparison with old results

In 2013 the big majority of 76 % replied within one business day or 24



Additonal 4% replied within 48 hours and 3 % replied within 72 hours, whereas 17 % did not reply in time.

Notice: automatic replies of e.g. ticket systems were not counted

Part 1 Interpretation of the results

In a strict interpretation we can say that 88 % (76 % in 2013) fullfilled the requirement to react within one business day - while 12 % (24 % in 2013) failed.

So we did better this time!

Is it good enough?

In a softer interpretation we can say that 95 % (83 % in 2013) are responsive while 5 % (17 % in 2013) are not.

So we have won 12 % ;)

How to deal with the last 5 %?

Part 1 CA's which could and should do better

CA	
BYGCA (BYGCA)	RESPONDED TO QUESTIONS after 7 days, though
DZeScience (0a49430a)	
DZeScience (DZeScience)	
EG-GRID (EG-GRID)	
INFN-CA-2006 (INFN-CA-2006)	
INFN-CA-2015 (INFN-CA-2015)	
KISTI-2007 (KISTI-2007)	
MARGI (MARGI)	
NECTEC (NECTEC)	
NERSC-SLCS (NERSC-SLCS)	
REUNA-ca (REUNA-ca)	
TSU-GE (TSU-GE)	

- INFN had problems with their email server that day some messages have been lost or were not delivered. The problem was solved at the site.
- Others will be contacted now or by their PMA-chair later...

Answers received within two business days
Answers received til and after end
Missing answers in the end

Part 2 The two additional questions

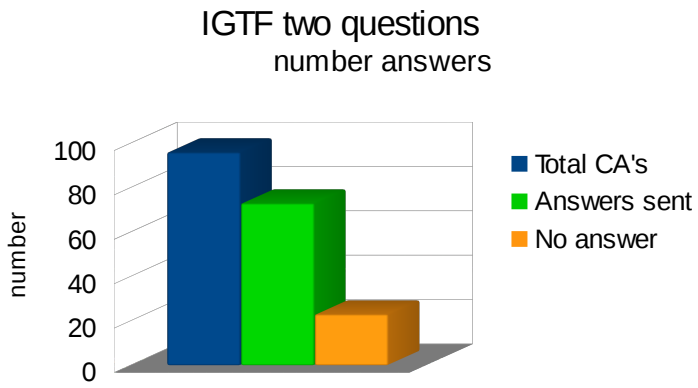
- Do you issue sha2 signed certificates by default?
- When is the last sha1 signed certificate going to expire?

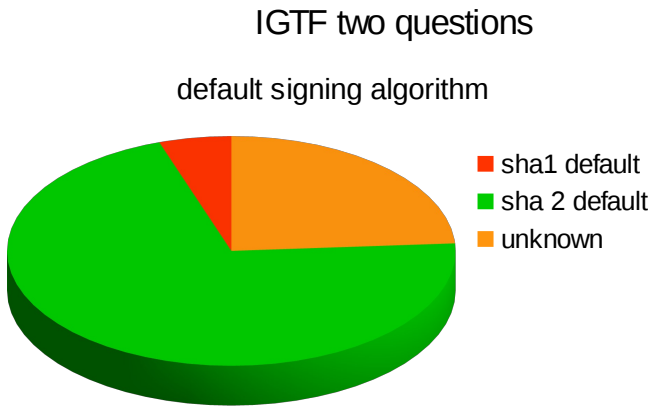
Part 2 rough summary (1)

- 73 CA's did kindly answer the questions (76 %)

  5 of them still issue sha1-signed certificates, the other 68 issue sha2 (sha256/sha512) by default

- 23 CA's did not sent answers (24 %)





Part 2 – CA's with sha1 default

CA	Q 1: Do you issue SHA-2 signed certificates by default?	Q 2: When will your last SHA1 signed certificate expire?
	Answer Q1	Answer Q2
BYGCA (BYGCA)	We proceed to issues SHA1 certificates because there is an infrastructure that depends on them.	
DZeScience (0a49430a)	Not yet.	Our CA certificate (issued with SHA-1) will expire 16 June 2026
DZeScience (DZeScience)		
FNAL-SLCS (FNAL-SLCS)	We do not yet issue SHA-2 certs by default, as we are still waiting for all cert users to test that their applications work with SHA-2. (We can switch the CA to issue only SHA-2 certs with very little notice if required)	We only issue short lived (one week lifetime) certs, so the last SHA-1 certs will expire one week after they are last issued.
RDIG (RDIG)	No.	10:35:38 UTC, 25/12/2016

Ursula.Epting@kit.edu

Part 2 rough summary (2)

- Several CA's have some sha1-signed certs which will all expire within 2016
- In Germany we have a special community for climate research which is not able to use sha2 and whishes to use sha1 forever.

Part 2 some details (3)

- Look on the complete table (not public, sorry)

The end

Thanks

Ursula.Epting@kit.edu