Fundação para a Computação Científica Nacional

Foundation for National Scientific Computing

Approach to DNSSEC by the use of Dynamic Updates

Eugenio Pinto & Sara Monteiro

eugenio.pinto@fccn.pt

sara.monteiro@fccn.pt

32nd International Public ICANN Meeting, 25 June 2008, Paris

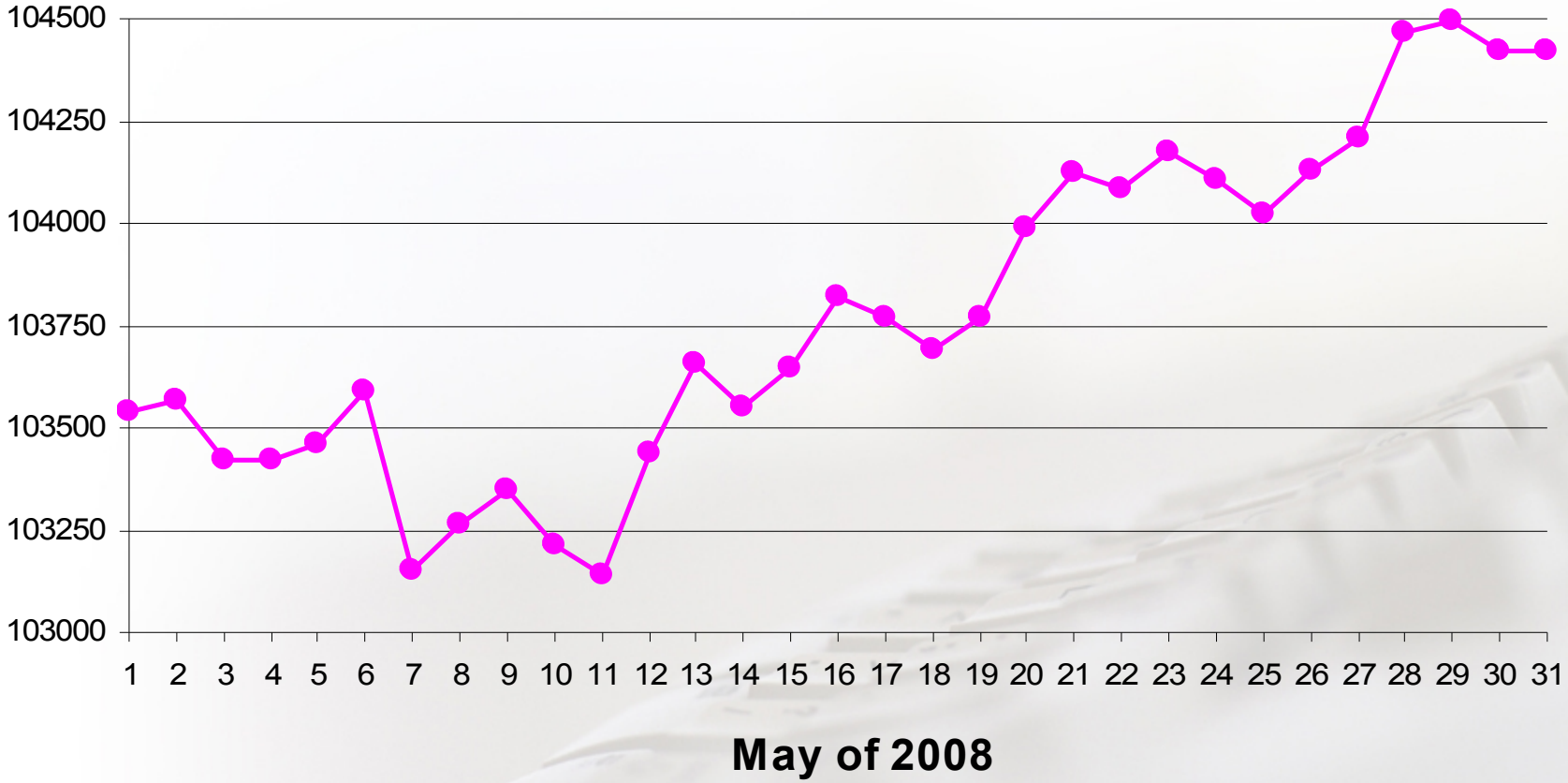
Purpose

- One of the concerns about implementing DNSSEC is the processing power consumption and time that is required to sign an entire zone file.

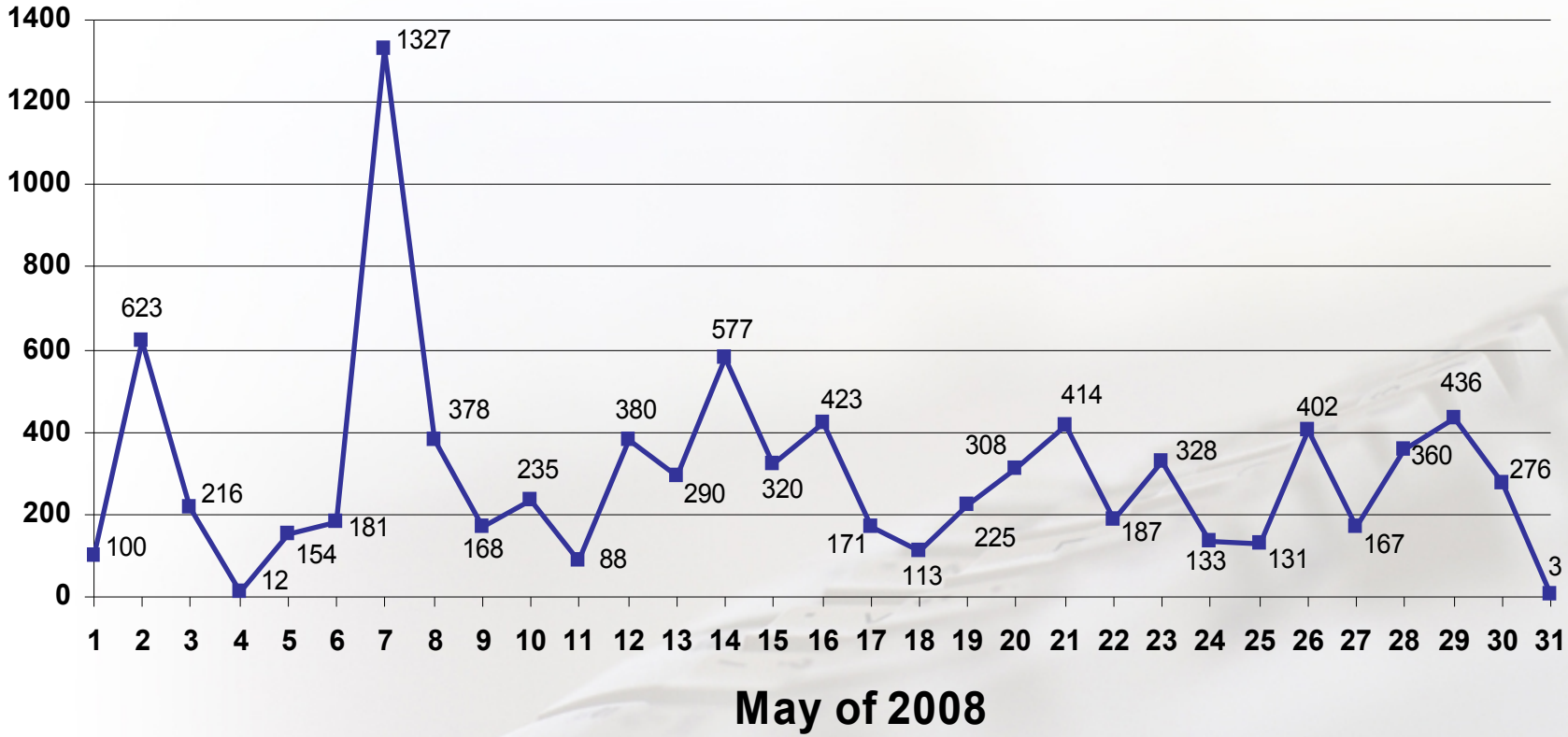
- This presentation shows how to put dynamic updates into the equation in order to reduce the amount of resources needed.

Fundação para a Computação Científica Nacional

Number of delegations in .PT zone



Domain updates



Let´s compare numbers

- Delegations in Zone: around 104.000
- Domain updates per day: around 400

Using the dnssec-signzone tool, everytime we do a full zone signing, we have to sign all the 104.000 delegations.

If we could sign just the updates…

Dynamic Updates

…but we can!

Doing dynamic updates in an already signed zone, Bind automatically signs every new resource record and updates the necessary NSEC resource records too.

So, we can save time avoiding re-signing resource records that were already signed, and in an easy way!

Full Zone Generation vs. Dynamic Updates

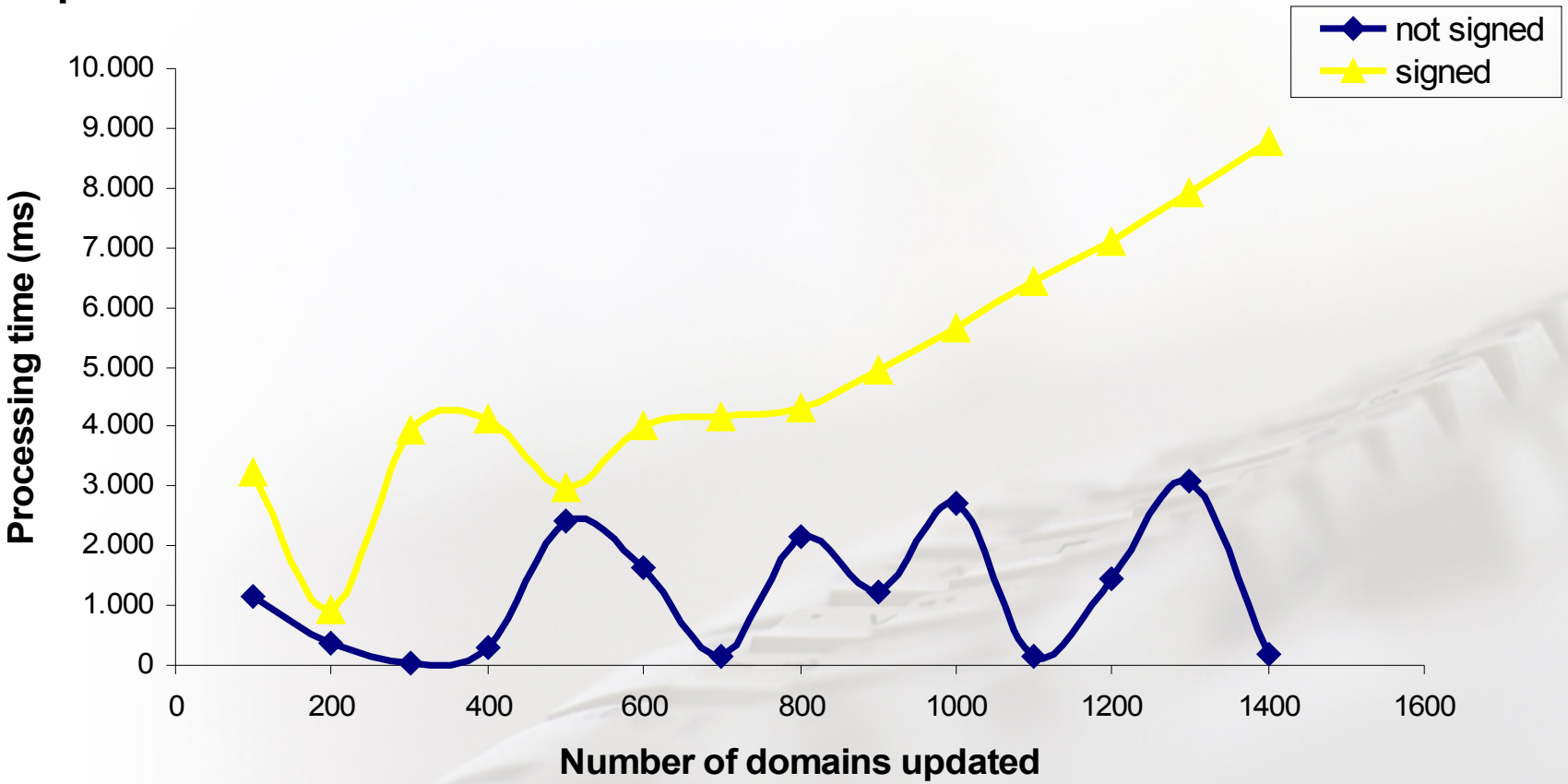
Time required to sign and install a new zone file, using full zone signing:

- Time to **build** the new zone file: 135.000 ms
- Time to **sign** the new zone file: 150.800 ms
- Time to **load** the signed zone file: 9.202 ms

Total time consumed: 295.002 ms (4 min 55 s)

Full Zone Generation vs. Dynamic Updates

Time required to send, sign and load dynamic zone updates in bulk:



Let´s compare numbers

- With full zone signing it is allways required near 5 minutes to do a unique delegation change.

- Using a single dynamic update request, in less then 5 seconds we can change up to 800 delegations in a signed DNS zone.

5 seconds is 1,7% of 5 minutes!

Precautions on using Dynamic Updates

So,

Dynamic Updates and signature on-the-fly solve the processing power consumption issue.

But doesn’t itself bring other concerns?

Precautions on using Dynamic Updates

Security:

- You should configure Bind to accept dynamic update requests only from your own machines and using a key that only you know;
- Additionally, you should enable dynamic updates to your zone just before you do a dynamic update and disable it right after.

Precautions on using Dynamic Updates

Key Roll-Over & Signatures Expiration:

- From times to times, you should sign the entire zone to renew the RRSET signatures as well as your public key(s);
- This can also be useful in the protection from any kind of undetected Dynamic Update failures.

DNSSEC Development Environment at .PT

DNSSEC main concerns:

- NSEC
- Key Roll-Over

NSEC

- In order to avoid zone walking, the DNSSEC Development Environment (as well as the DNSSEC EPP features) will only be available for our Registrars after a successful NSEC3 patch is applied to the Bind server.

Key Roll-Over

- The key roll-over procedure is a critical point in the DNSSEC implementation. We will use very short TTLs in our tests in order to analyze risks and timely mitigate them;
- For the same purpose, our development DNSSEC server will also be fed by our live data and Middleware (with the new features in parallel) for a while before it is put in production.

Questions & Answers

Now that you have the tools and know how to use them, will you make use of them?

eugenio.pinto@fccn.pt
sara.monteiro@fccn.pt