

The IRT-Object in the RIPE Database: short status update (and some background)

Wilfried Wöber: ACOnet-CERT

for TF-CSIRT, 17th Meeting – Amsterdam, NL

January 23, 2006



What happened since last update?

- Some general ideas to return “less” email addresses on default queries have been implemented (success!!)
- References to X.509 objects are supported
- Decision taken during most recent RIPE Meeting to include IRT data on “simple” **whois** queries (as it was meant to work...)



On a more general note...

- Security provisions protecting database transactions have been improved already (already removed “**none**” and “**mail-from**”)
- Proposal to phase out **crypt-pw** is in the works (target date: RIPE52 Mtg. in Istanbul)
- This will leave us with **crypt-md5** (legacy), PGP and X.509 (recommended)



A question for the community

- How many (european region) teams are aware of this mechanism?
- How many teams do have “direct” links to LIR(s) in the first place?
- How many CERTs do use this already
- Any follow-up required, like training?
- AOI (any other input)

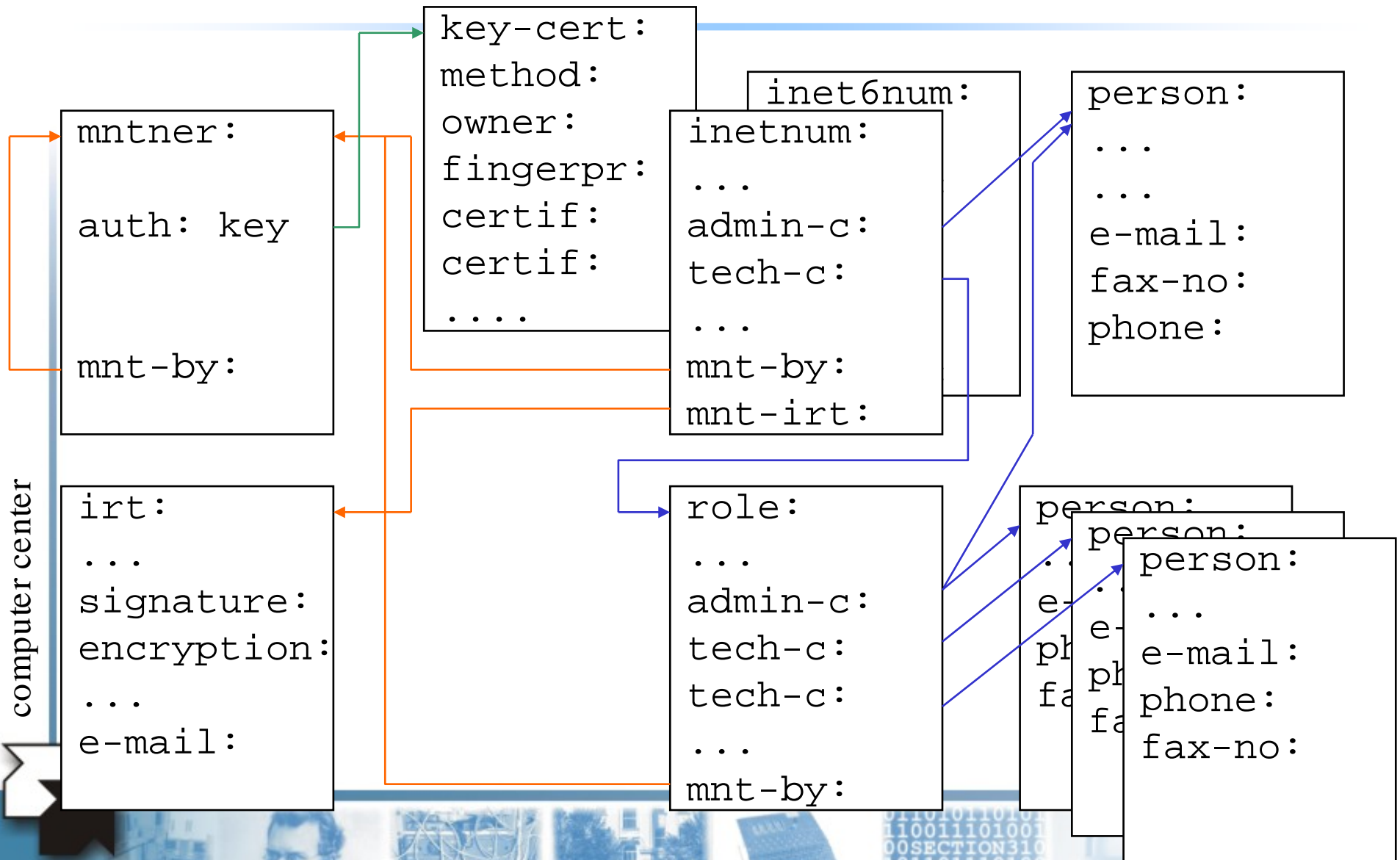


What does the IRT-Object do?

- Documents existence of **I**ncident **R**esponse **T**eams in the RIPE Database
 - Registers contact information: PGP-Keys, ...
- Links to address objects (inetnum, inet6num)
- Supports a more fine grained and scalable approach (and hierarchy) than individual 'abuse-mailbox' entries
- Only one (or very few) object(s) need(s) maintenance



Relationship between DB objects



What does it look like?

```
irt:           IRT-JANET-CERT
address:       Atlas Centre
address:       Chilton
address:       DIDCOT, Oxon
address:       OX11 0QS UK
phone:         +44 1235 822 340
fax-no:        +44 1235 822 398
e-mail:        cert@cert.ja.net
signature:     PGPKEY-836D7141
encryption:    PGPKEY-836D7141
admin-c:       AB2554-RIPE
tech-c:        RT644-RIPE
auth:          PGPKEY-3EA2BD2B
remarks:       JANET-CERT coordinates security in JANET.
remarks:       http://www.ja.net/cert/
remarks:       JANET is the UK education and research network.
irt-nfy:       ripe-admin@cert.ja.net
notify:        ripe-admin@cert.ja.net
mnt-by:        JANET-CERT
changed:       cert@cert.ja.net 20020808
source:        RIPE
```

Team's PGP-key used for signing

Team's PGP-key used for encryption

Team's PGP-key used to authenticate references

eMail Address to notify about references

vienna university
computer center



.

Questions

