Early Warning System - CIRCA

Computer Incident Response

Coordination Austria

Rudolf SCHRAML

Early Warning System - CIRCA

What is this all about...

- A public - private partnership project (PPP) between
  - BKA: Bundeskanzleramt (Federal Chancellor's Head Office)
    - coordinating the public sector
    - coordinating the critical infrastructure in Austria
  - ISPA: Internet Service Providers Austria
    - coordinating the Internet Service Providers in Austria
- A name and an umbrella for various activities
  - deals with worms, viruses, DDoS, trojans, phishing attacks, attacks against the core
  - tools, policies, framework for crisis management
  - human networking and information exchange

Early Warning System - CIRCA

- A „**Web of Trust**“ between

  - **BKA**
    - Government agencies, Critical Information Infrastructures and Social Partners (economic interest groups)
  - **ISPA**
    - (big) Commercial ISPs
      - membership is offered to key individuals, representing (the interests/activities of) an organisation
    - the NREN, Internet eXchange point(s)

      - well-defined policy for participation

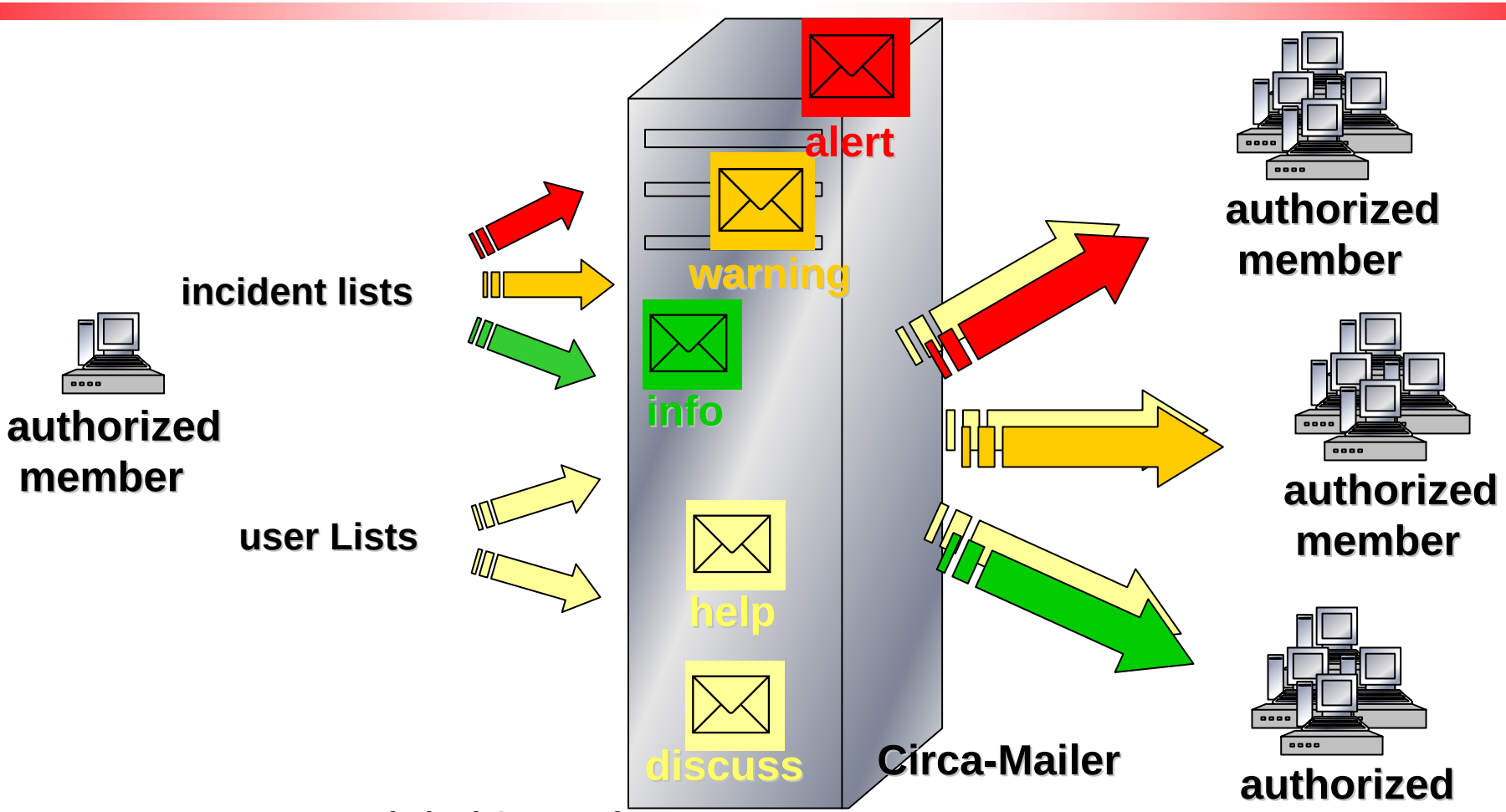
        (- only core operations and/or security staff which indeed can act "immediately" in case of incidents
        not: sales, helpdesk, PR or non-tech management
        - personal signature on documents required
        - counter-signed by employer, ISPA membership
        - non-disclosure, code of conduct
        - information not to be used for competitive advantage
        - responsibility to report changes in function or employment)

Early Warning System - CIRCA

A „Secure communication“ between the private and the public part

- 2 Mailing List Hubs
  - 1 for the private sector, 1 for the public sector
  - secure operational environment
  - manual forwarding of relevant information between clouds

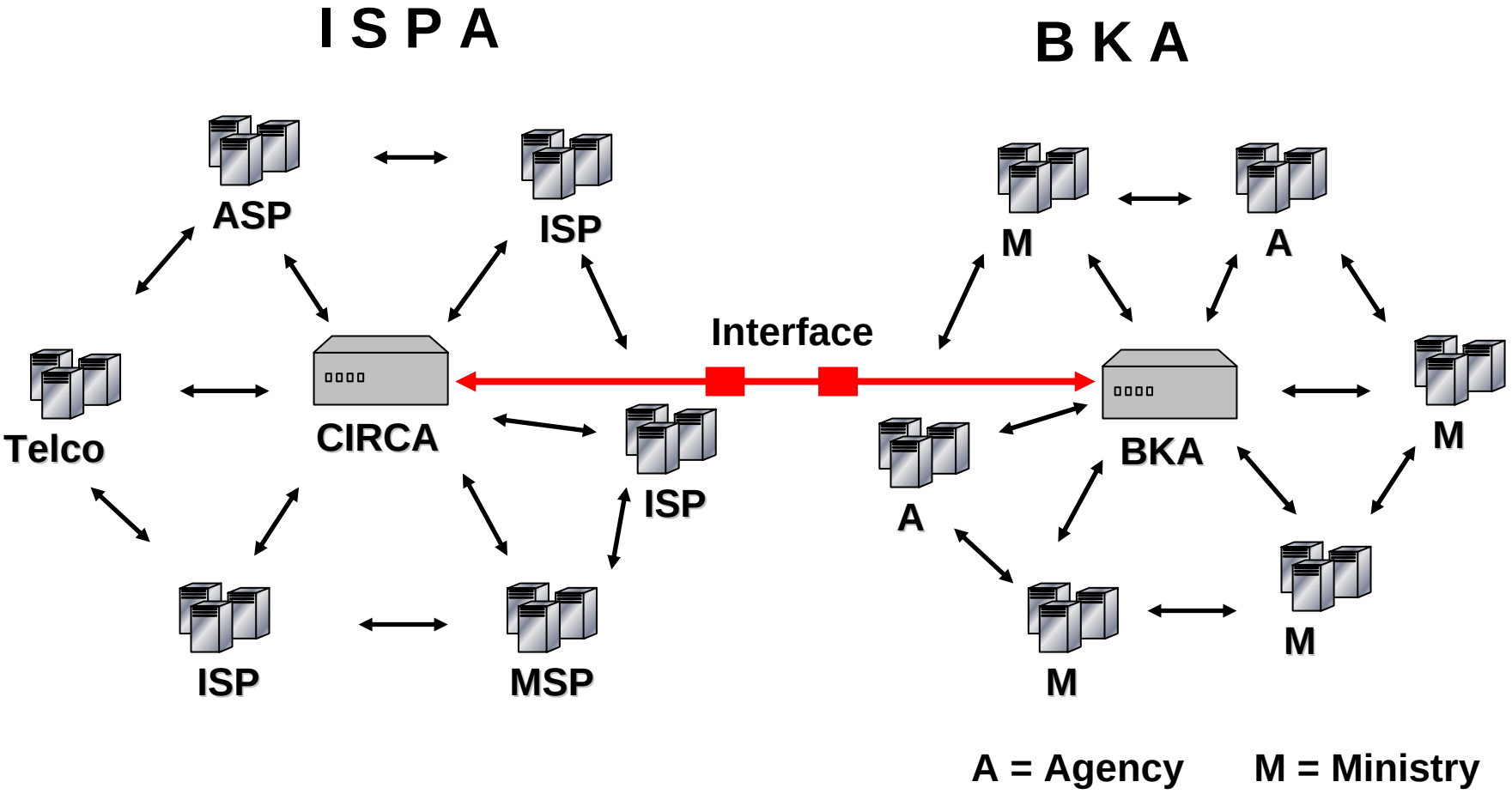
- Based on "Sympa" Mailer
  - Verification of sender's signature ***and*** encryption
  - X.509 ***and*** (eventually) PGP support, inter-working!
  - Archive
  - Subscription approval (for non-public part) by ISPA secretariat



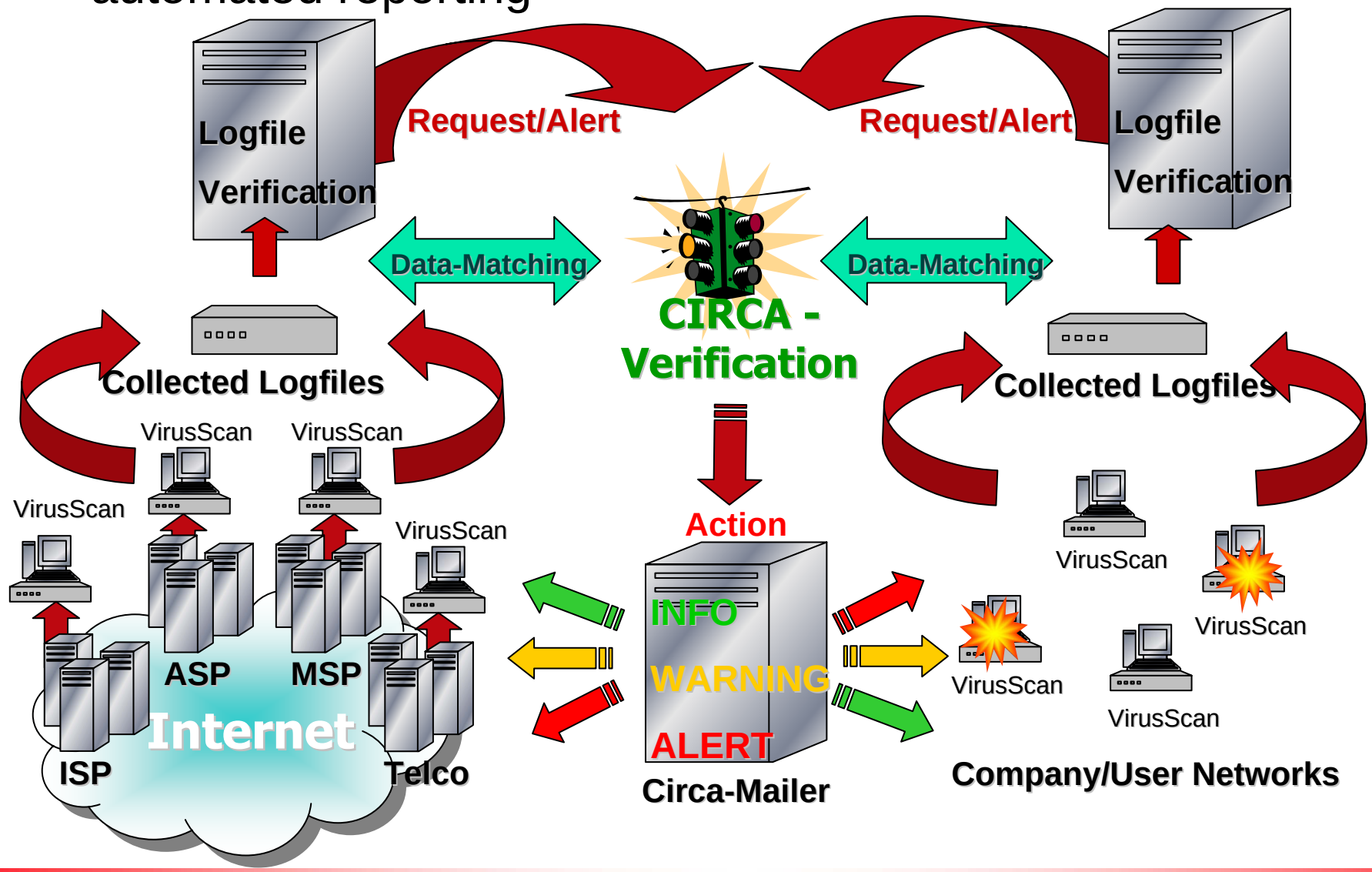
authorized member = Limited Group of Security-Admin of Infrastructure Networks, Security-Admin of ISP Security-Staff of Private Companies =

Web of Trust

Public Private Partnership



automated reporting



Early Warning System - CIRCA

- An Emergency / Crisis Management Team (“Krisenstab”)

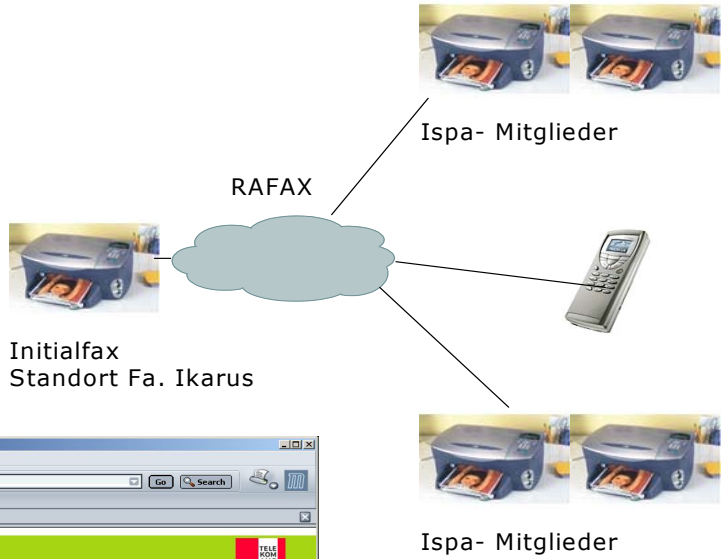
  - Contact details (confidential)
  - Individuals from different environments

  - **Procedures for**
    - Detecting and declaring an emergency
    - Coordination of press releases and external contacts
    - Physical meeting if necessary

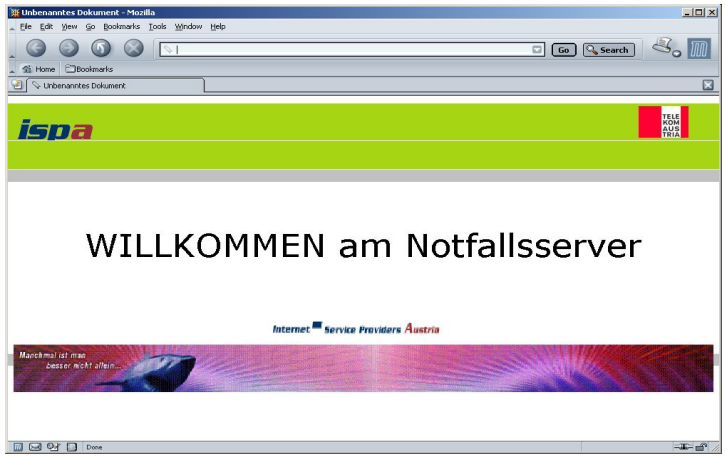
  - **Out of Band emergency server (patches,…)**

Emergency Communication and -server

automated Telefax
and SMS
information



Out of Band
emergency server
(ftp / Dial-up)



Early Warning System - CIRCA

Lessons learned: problems

- Acquisition and management of X.500 certificates can be a major pain
  - local, reliable source vs. ease of use in end systems
  - cost of certificates vs. expiration
  - installing certificates into different (versions of) applications and operating systems can be nontrivial
  - Everything takes 3 times as long as expected to get set up correctly and reliably :-(
- Provisioning of emergency management components requires a "real" commitment!
- Sandbox, pencil and paper, and mental exercises are OK, but you need regular fire-alarm training!
- Admission procedures for participation need on-going review, who decides/manages trust?

Early Warning System - CIRCA

Lessons learned: the good stuff

- X.509 and PGP inter-working on the lists is a big bonus
  - provides another aspect of flexibilty to accommodate company “rules”

- Exchange of information
  - on the lists (help, discuss, info, warning, alert)
  - during meetings (Round Table Events)

- Provides marketing advantage for the participants

- Improves communication between private and public sector

- General increase of security awareness

- Cross-Border Information-Exchange with other countries

Early Warning System - CIRCA

Current Activities:

- Types of Incidents seem to evolve
  - many defense technologies against worms and viruses are available these days, including early warnings
  - managed mail services become popular
- Is it going to help with completely new 0Day-Incidents?
  - we will see, eventually
- Social Engineering/Phishing Attacks become more sophisticated and more commonplace
  - activity and mandate of group changes over time
  - we have to integrate entities with
    - a different mind-set
    - or a different operational model

Early Warning System - CIRCA

Current Activities: continued

Today there is an Austrian promotion program for **security research** (short „KIRAS Programme") which supports national research projects whose results contribute to increase Security as a means of permanent guarantee of a high standard of living and opportunities for development for all members of a society. In the KIRAS program the term security research is defined in a multidimensional, long-term, multidisciplinary and integrative way. At the beginning a thematic focus on the promotion of projects concerning protection of **critical infrastructure** will be set.

In this Austrian promotion program for **security research** many CIIP projects have been started and not only the austrian government but also the critical infrastructures and the austrian economy is involved.

Early Warning System - CIRCA

Thank you for your kind attention!

- Questions or Comments?

Contact Information:

Rudolf Schraml
Bundeskanzleramt
I / B / 2 – IKT Strategie des Bundes
Ballhausplatz 2
1014 Vienna
AUSTRIA

rudolf.schraml@bka.gv.at
+43 1 53115 5423