# Public Key Cryptography from the point of view of an Infosec Agency

Ansgar Heuser (BSI)

# Does anyone really need public key cryptography?

– classical key management systems and authentication procedures based on symmetric algorithms are quite convenient to closed user groups (like military networks)

– nevertheless: public key cryptography is attractive!

# Are we able to master public key cryptography?

– the decade long tradition in development and evaluation of symmetric ciphers turned out to be more or less useless

– new people having enough background in e.g. algebraic number theory had to be brought in

# A proprietary public key system?

- for some idiosyncratic reasons infosec agencies always preferred proprietary solutions

- but this time all the efforts failed eventually

# Is there anything better than RSA?

## Yes: ECC

## (for the well known reasons)

# How do we handle ECC today?

- wherever in our projects public key cryptography
makes sense we will base it on ECC

- logarithmic group size: round about 256 bits

- the curves are found by counting their points

# How do we handle ECC today?

- current preeminent projects:

  – ISDN equipment (ELCRODAT 6–2)
  – universal crypto controller (PLUTO)

- our recommendations of algorithms for digital signatures include RSA as well as ECC

# How long will we survive with ECC??

- „the principle of hope“:
  for the time being nobody expects a dramatic breakthrough

- in real life implementations we try to introduce an extra margin of security