SWITCH

The Swiss Education & Research Network

SWITCHpki - looking back and ahead

Security targets

SWITCH
The Swiss Education & Research Network

P Privacy

A Authenticity

I Integrity

N Non-Repudiation

How PKI fits into the picture

SWITCH
The Swiss Education & Research Network

Serverside PKI

- **P, I**: encryption and checksums
- **A**: provides server identity assurance to the user
- **N**: online relevance only, assurance does not extend beyond session
- Industry standard solution for e-commerce since years
- Operational service SWITCHpki since March 2004

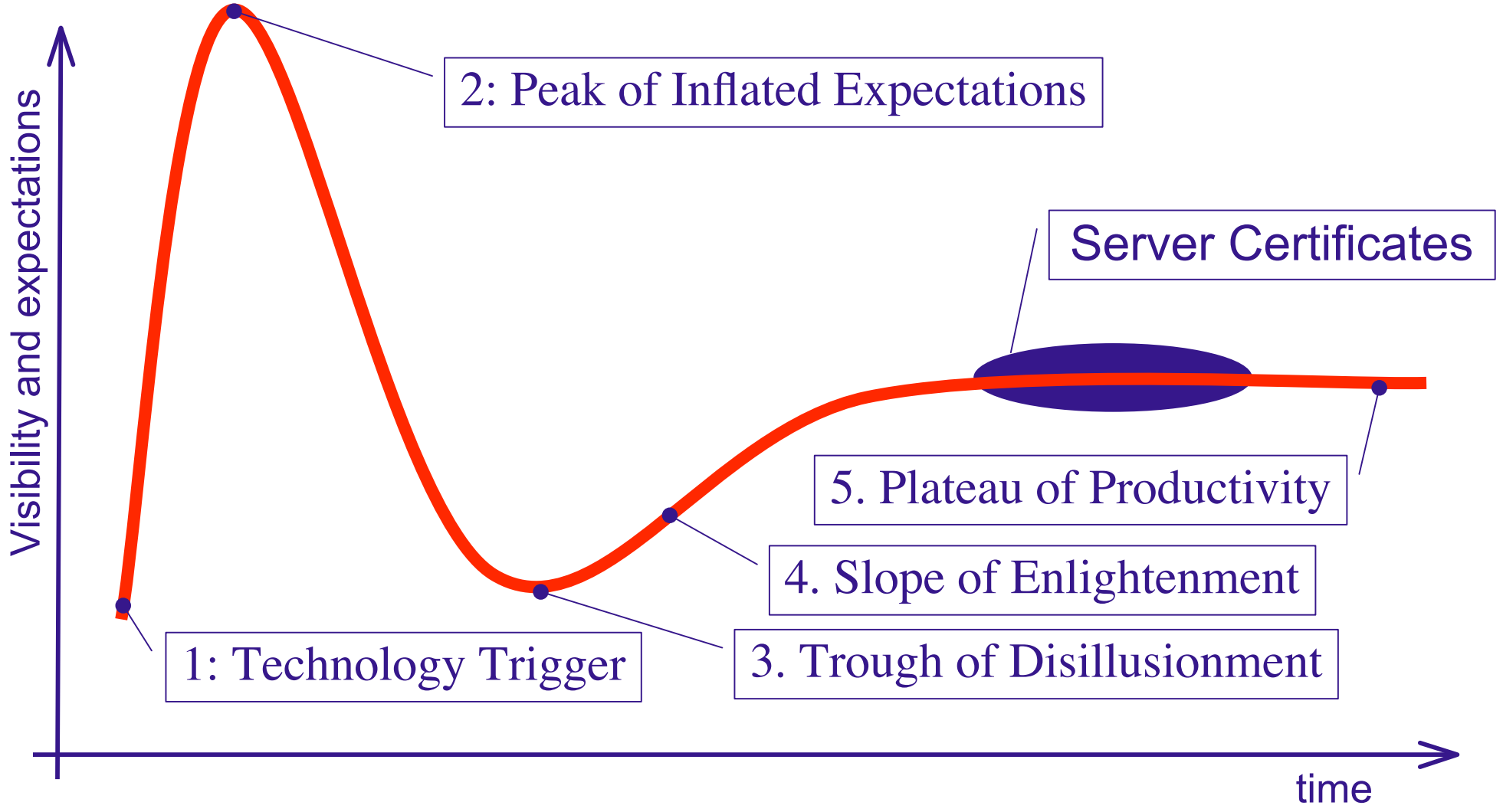
Clientside PKI

- **P, I**: encryption and checksums
- **A**: provides user identity assurance to the server
- **N**: electronic signature
- Only little relevance outside closed communities
- Little demand, pilot service since end 2005

Hype Cycle - Straight from the books

SWITCH
The Swiss Education & Research Network

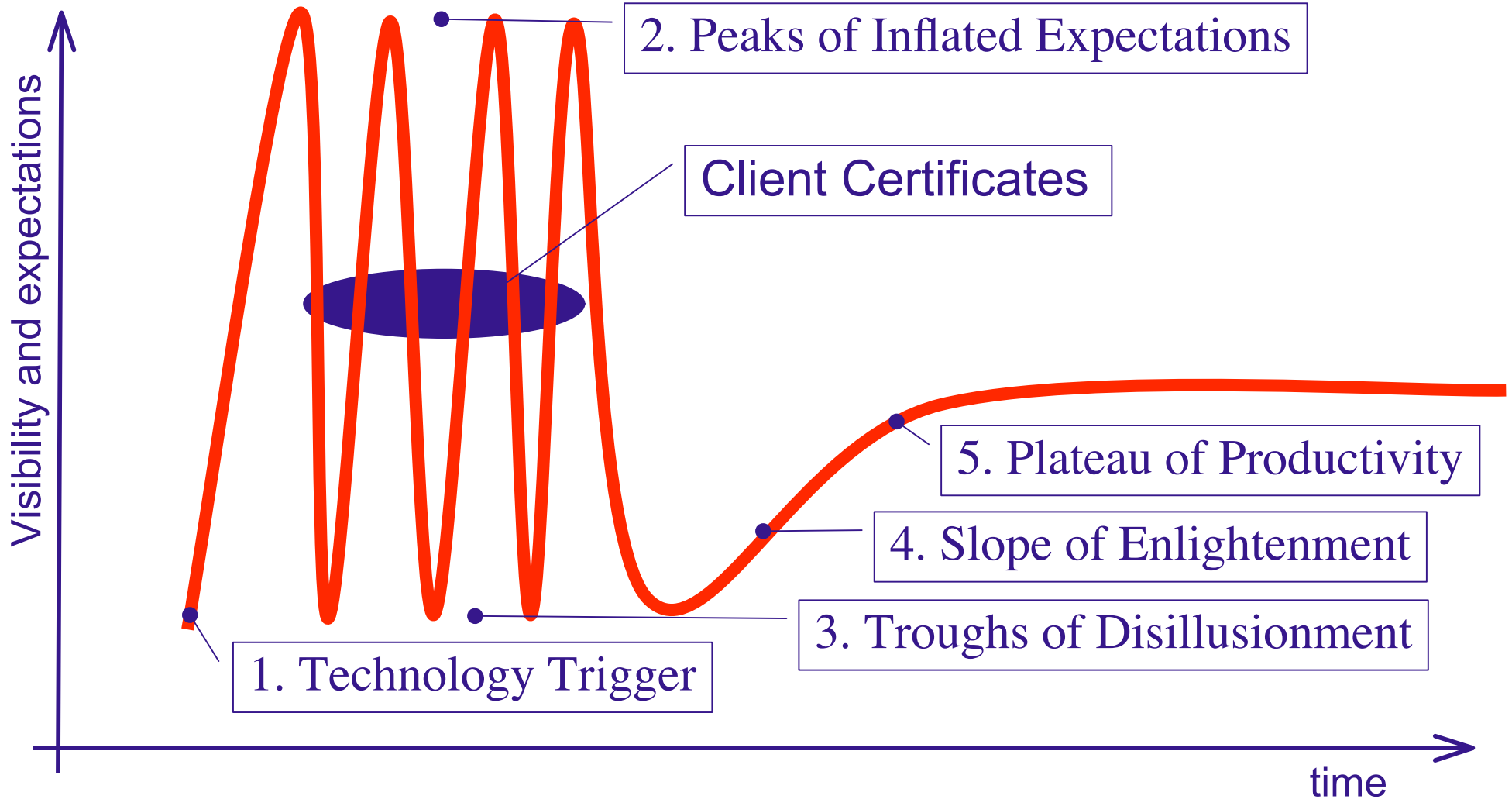
Source: http://www.gartner.com/pages/story.php.id.8795.s.8.jsp



Hype Cycle - The client cert way...

SWITCH
The Swiss Education & Research Network

Source: http://www.gartner.com/pages/story.php.id.8795.s.8.jsp

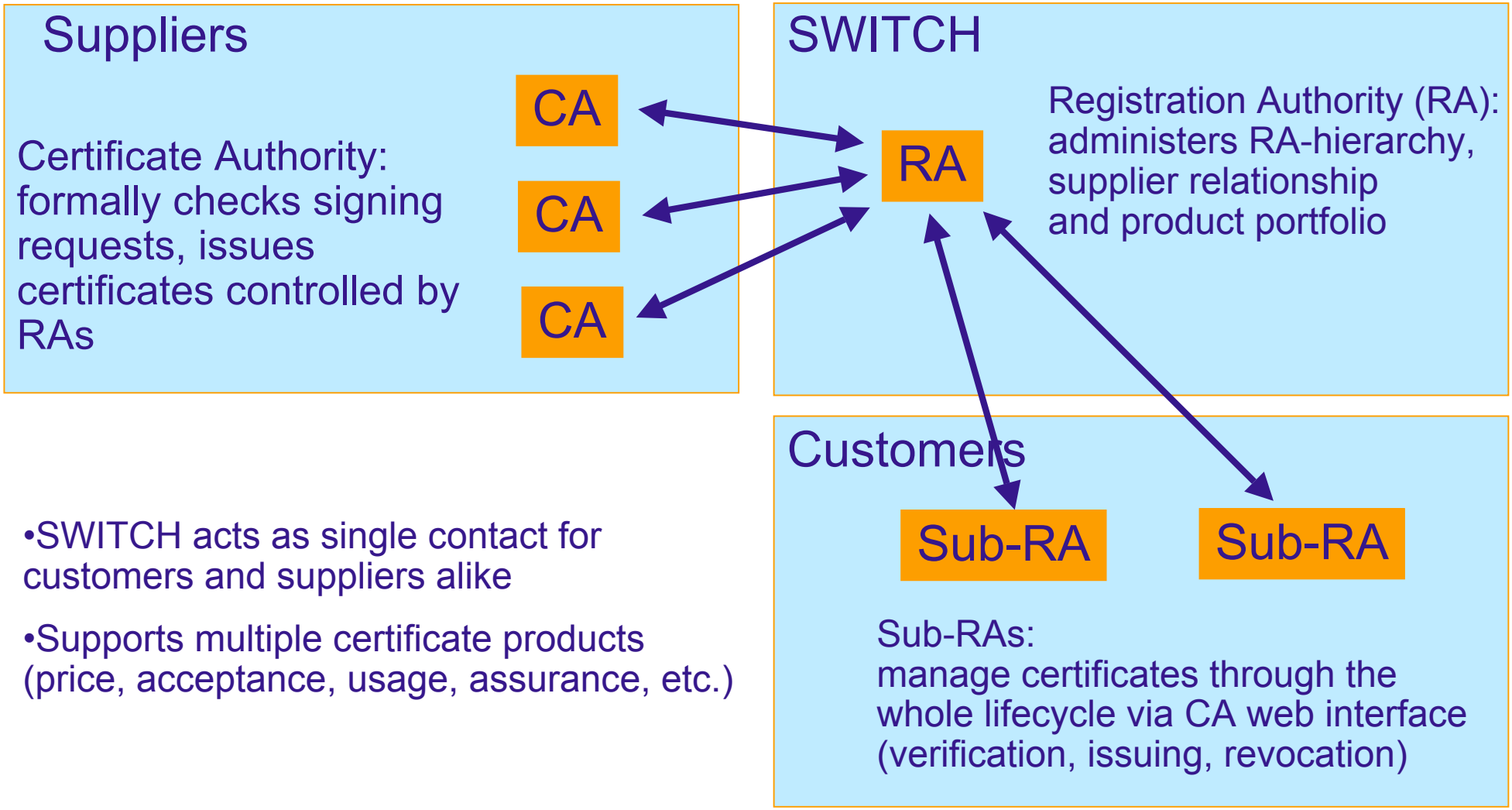


SWITCHpki service concept

SWITCH
The Swiss Education & Research Network

Technical components

Organisational components



- SWITCH acts as single contact for customers and suppliers alike
- Supports multiple certificate products (price, acceptance, usage, assurance, etc.)

Some figures

SWITCH
The Swiss Education & Research Network

SWITCHpki participants (organisations): 20

- SWITCHpki Basic: 18
- SWITCHpki Extended: 2

Valid SWITCHpki certificates in the wild: 290

- Server certificates: 275
- Client certificates: 15

Our next steps...

SWITCH
The Swiss Education & Research Network

- Improving the certificate service
  - Cheaper (e.g. through economy of scale à la SCS)
  - Easier to manage (preinstalled root certs, improved RA interface)
- Help maturing client certs (Slope of Enlightenment)
  - Client cert pilot cases
- Bridge the two worlds: AAI and PKI
  - Free the synergies in the overlap
- Learn from PKI
  - Add “assurance” to AAI
- Learn from AAI
  - How about: Getting your certificates through AAI?

The Swiss Education & Research Network