A Demonstrative Ad Hoc Attestation System

ISC 2008

Taipei, Taiwan

16th -18thof September 2008

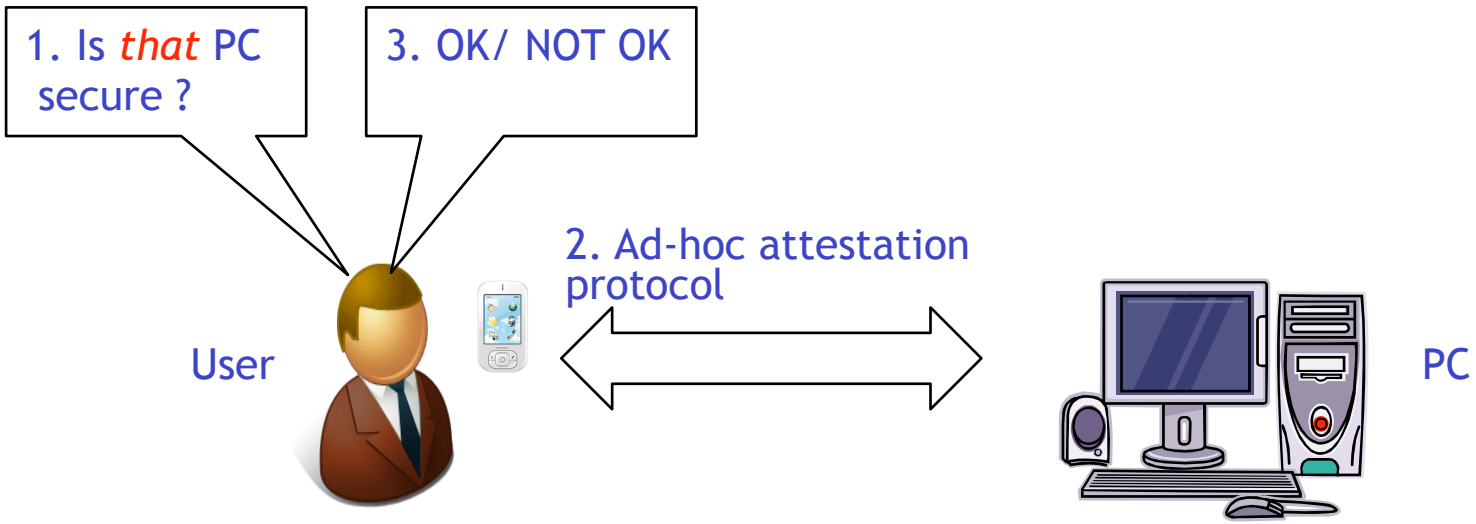
Endre Bangerter[1], Maksim Djackov[1] and Ahmad-Reza Sadeghi[2]

[1]Bern Univ. of Applied Sciences, Switzerland
and
[2]Univ. of Bochum, Germany

Agenda

- Demonstrative ad hoc attestation – idea and challenges
- Token technology
- Our ad hoc attestation system
- Conclusions

Goal of demonstrative ad-hoc attestation



Potential application scenarios of ad-hoc attestation:

- Kiosk computing / Internet cafes
- Check your office mate's PC, home PC, your own PC etc before using it for critical tasks
- Check an ATM before using it

"Demonstrative": PC to be attested is identified physically by user.

- That is, PC is identified "by pointing at it", not through certificates etc.

"Ad-hoc": No pre-shared PC specific information necessary. E.g.,

- No pre-shared keys btw. PC and handheld
- No ID-string of PC available
- Etc.

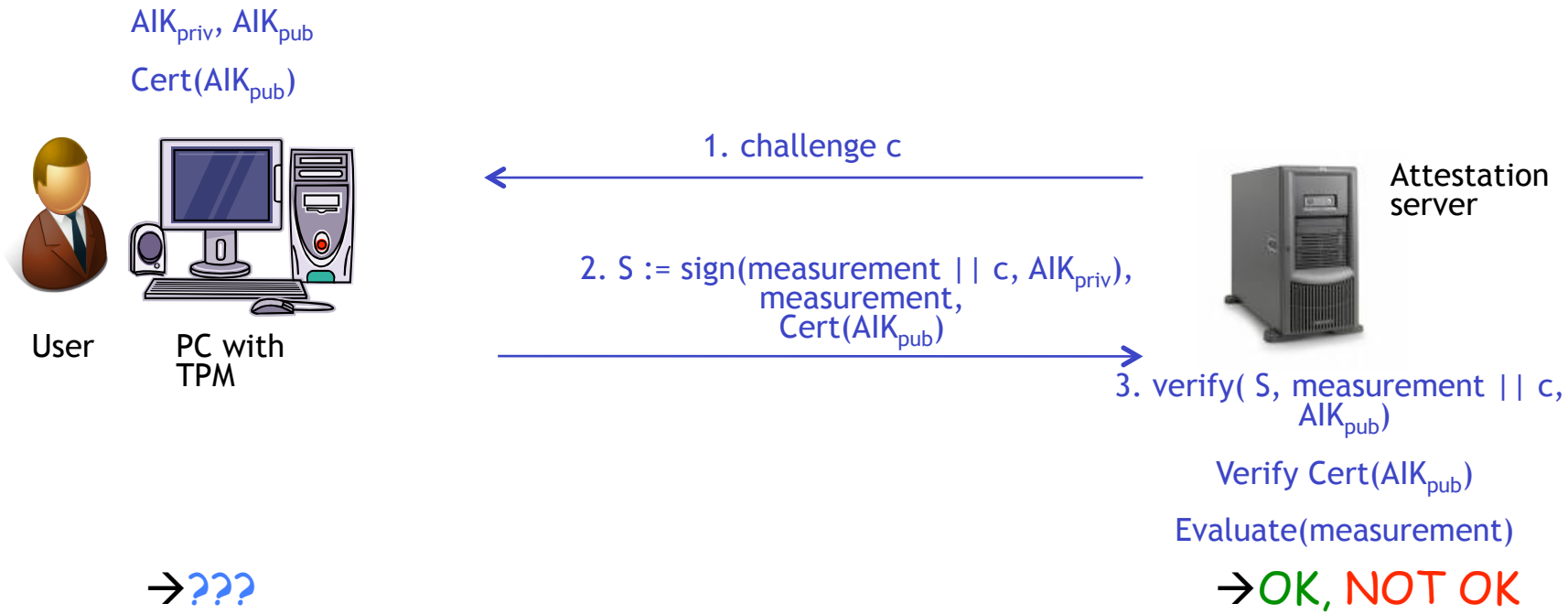
Trusted computing

- *Trusted computing group (TCG)* is an industry consortium with the mission to "enable more secure computing environments without compromising functional integrity, privacy, or individual rights."

- *Trusted Platform Module (TPM):* Trusted chip built into many PCs & laptops. Idea is to extend from TPM to entire platform (e.g,. OS etc.)

- *Operations provided by TPM:*
  - Storage of platform integrity measurements (i.e., hashes of files)
  - Signing of platform integrity measurements
  - Generation of various keys, e.g., symmetric encryption keys
  - Encryption & decryption
  - Etc.

Trusted computing - Remote attestation

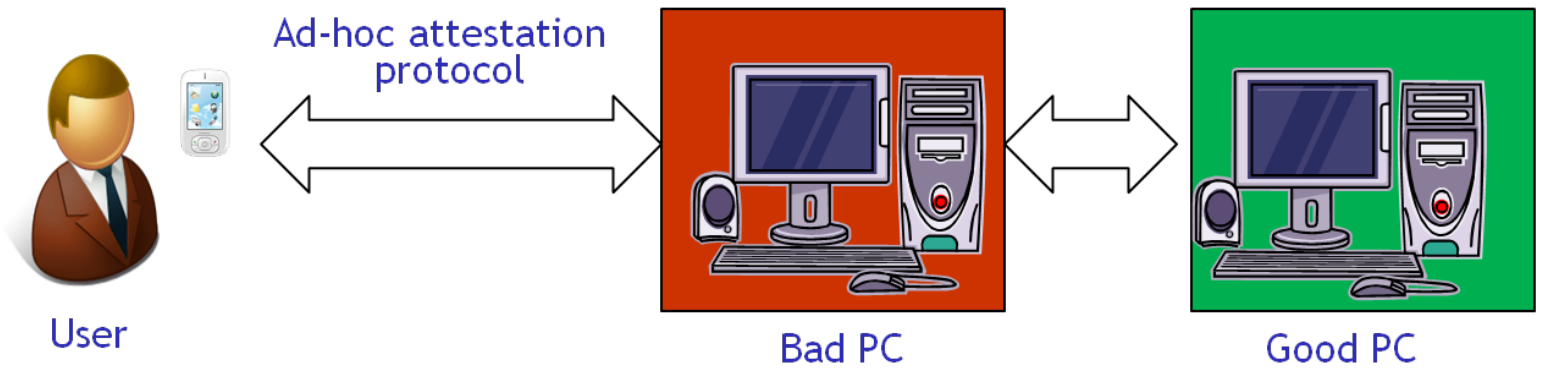


- Server learns whether User PC is trustworthy
  - Adequate in many scenarios, e.g., verify client before connecting to company intranet
- Is not meant to improve the user's trust in the client platform
- Is not a solution for "demonstrative ad-hoc attestation"

Open ad-hoc attestation challenges

Perrig et al. Turtles all the way down: Research challenges in user-based attestation. Usenix Hot Topics in Security 2007.

- Platform in the middle attack:



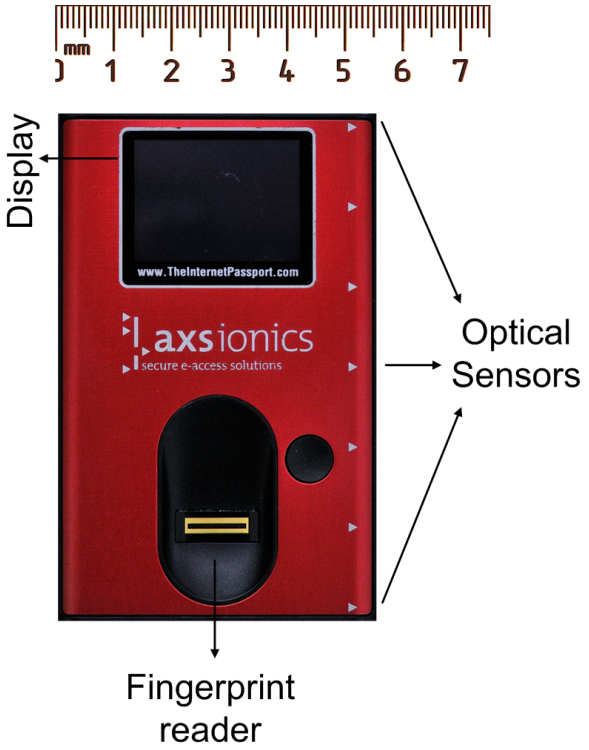
- Usability & viability:
  - User device: affordable, commodity hardware, small form factor
  - Universal connectivity between the user device and the target platform → any platform can be ad-hoc attested
  - User device itself has to be trustworthy and resilient against attacks
  - Device and the ad-hoc attestation protocol shall be intuitive and easy to use
- Management and evaluation of integrity measurements:
  - Store DB of known good integrity measurements on handheld? How to keep up to date?

Agenda

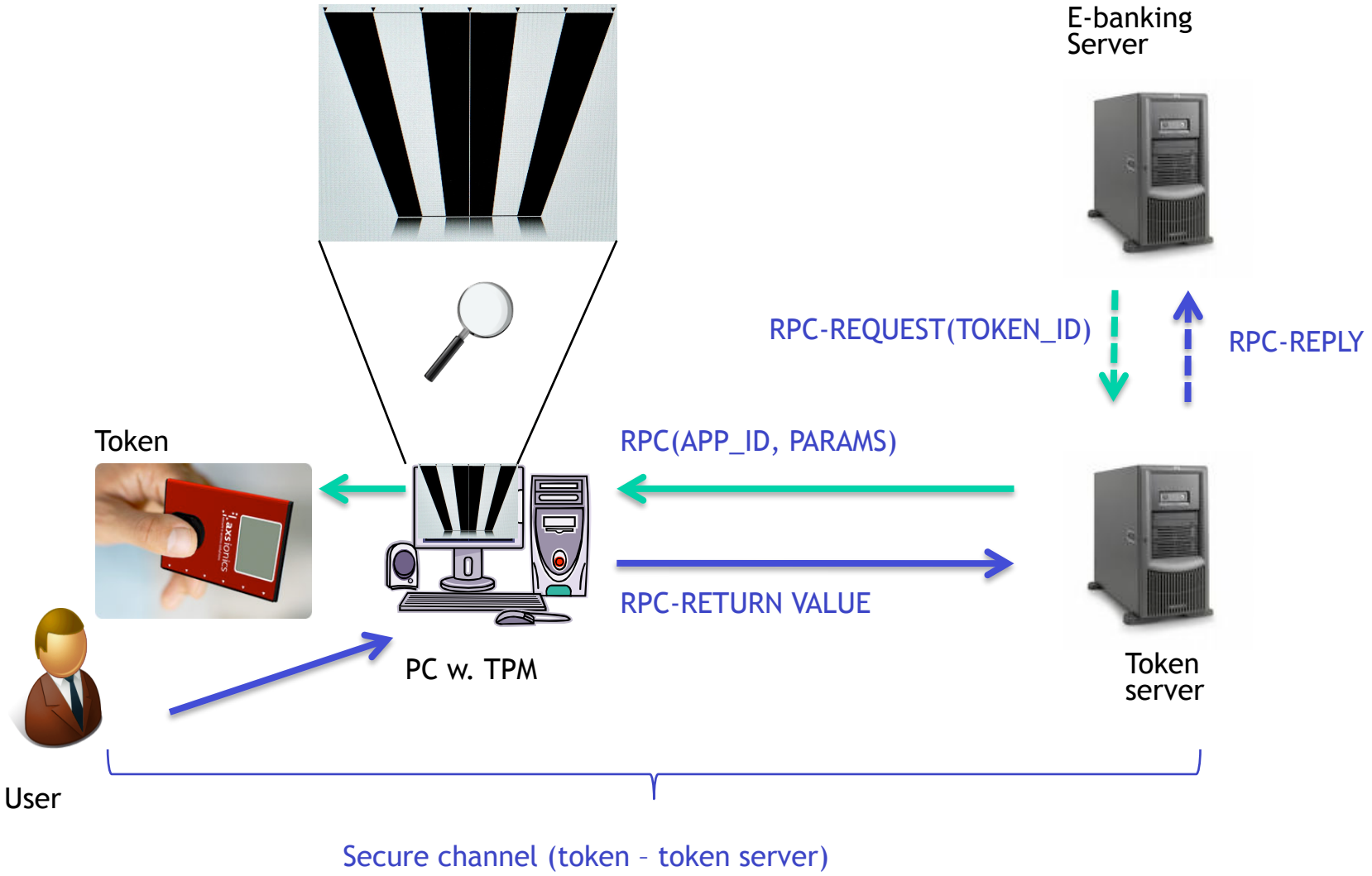
- Demonstrative ad hoc attestation – idea and challenges
- Token technology
- Our ad hoc attestation system
- Conclusions

AXSionics Token

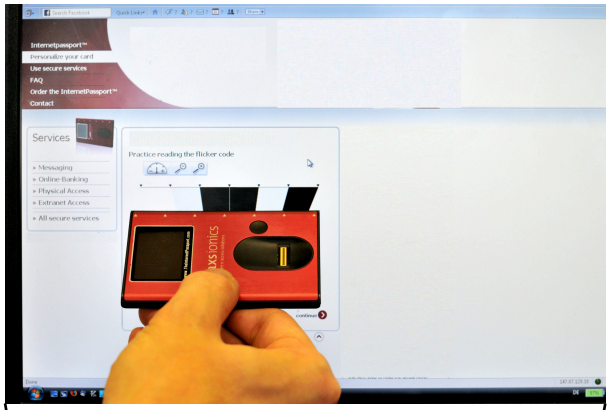
- Our ad-hoc attestation system makes essential use of a novel security token technology
  - Essential for usability and security
- Token technology was made available to us for research purposes by AXSionics
- Key features of the token:
  - Roughly smart card sized
  - Optical interface (to read of data from a computer screen)
  - Display (128 * 96 pixels)
  - Fingerprint reader for logon and navigation on display
  - Secure execution architecture (all computation and storage inside ARM secure core CPU, custom firmware)



Security token functionality and architecture (1/2)



Security token functionality and architecture (2/2)



E-banking Server

RPC-REQUEST(TOKEN_ID)

RPC-REPLY

Token

RPC(APP_ID, PARAMS)

RPC-RETURN VALUE

Token server

User

Secure channel token – token server

Flickering demo

http://axsportal.com

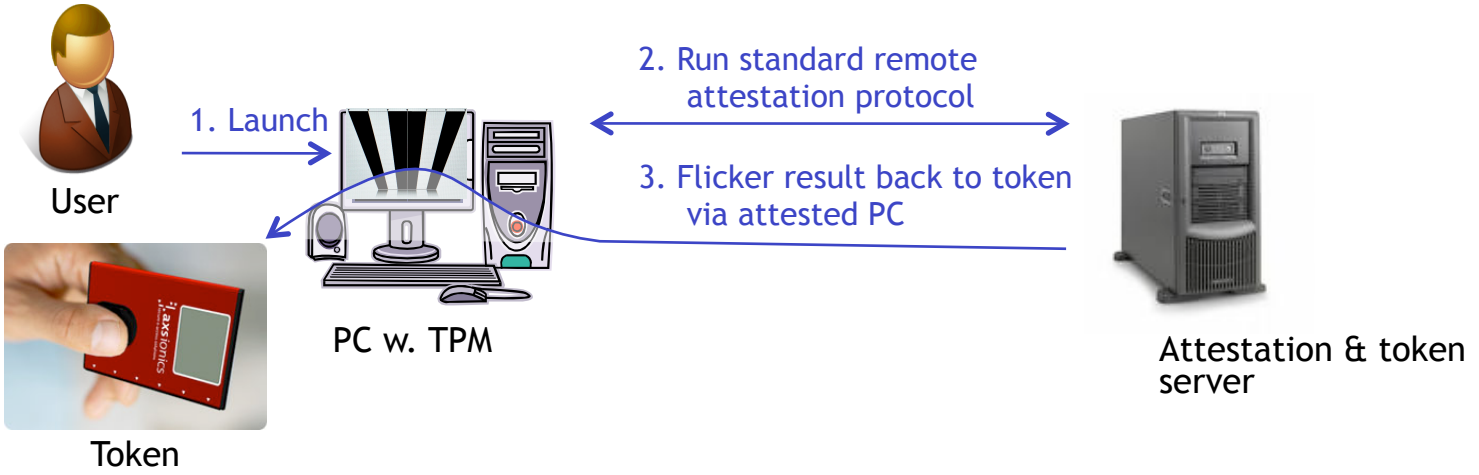
Agenda

- Demonstrative ad hoc attestation – idea and challenges
- Token technology
- Our ad hoc attestation system
- Conclusions

Our ad hoc attestation system - Usage perspective

- Intuitive usage paradigm: "Hold token to the screen of the PC to be attested"
- Usability & viability (challenges from Perrig et al.):
  - ☑ User device: affordable, commodity hardware, small form factor
  - ☑ Universal connectivity between the user device and the target platform → any platform can be ad-hoc attested
  - ☑ User device itself has to be trustworthy and resilient against attacks
  - ☑ Device and the ad-hoc attestation protocol shall be intuitive and easy to use
- Usage paradigm inherited from the token technology

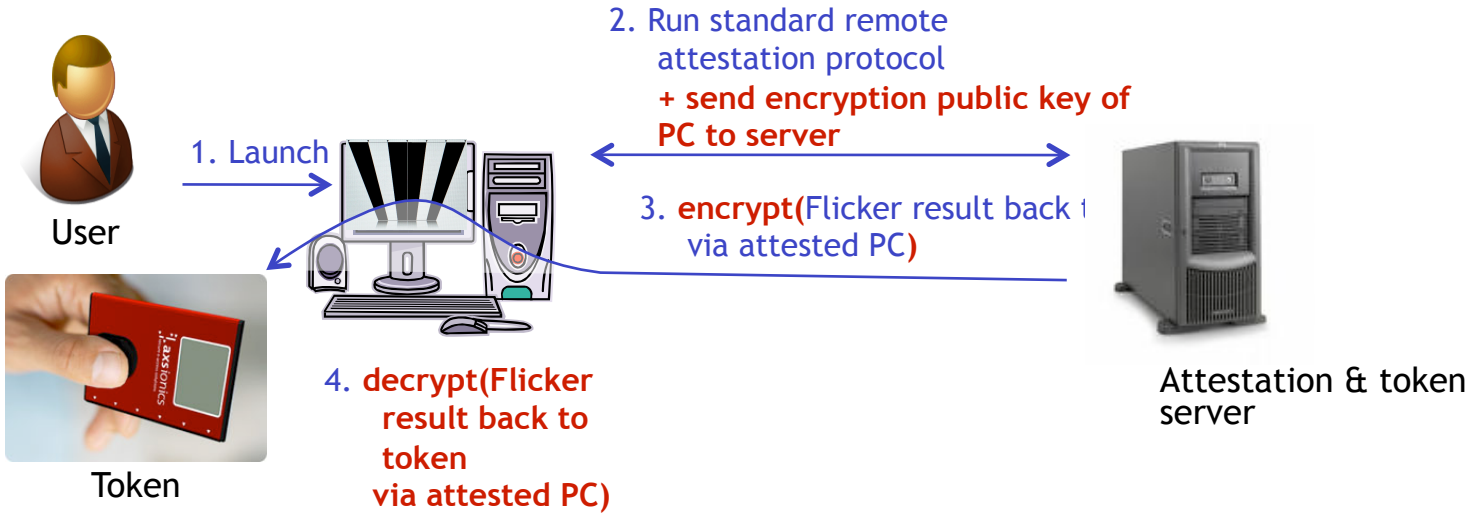
Our ad hoc attestation system – Basic idea (1/2)



- Security considerations:
  - Secure channel between attestation & token server and token → token as secure display of server towards user
  - Still vulnerable to platform in the middle attack: message 3. containing "flickering" can be deviated to malicious platform
- Server based architecture:
  - Attestation is offloaded to server
  - No logic and measurement details need to be maintained on token
  - Attestation can be offered as a service (e.g., like virus signatures today)

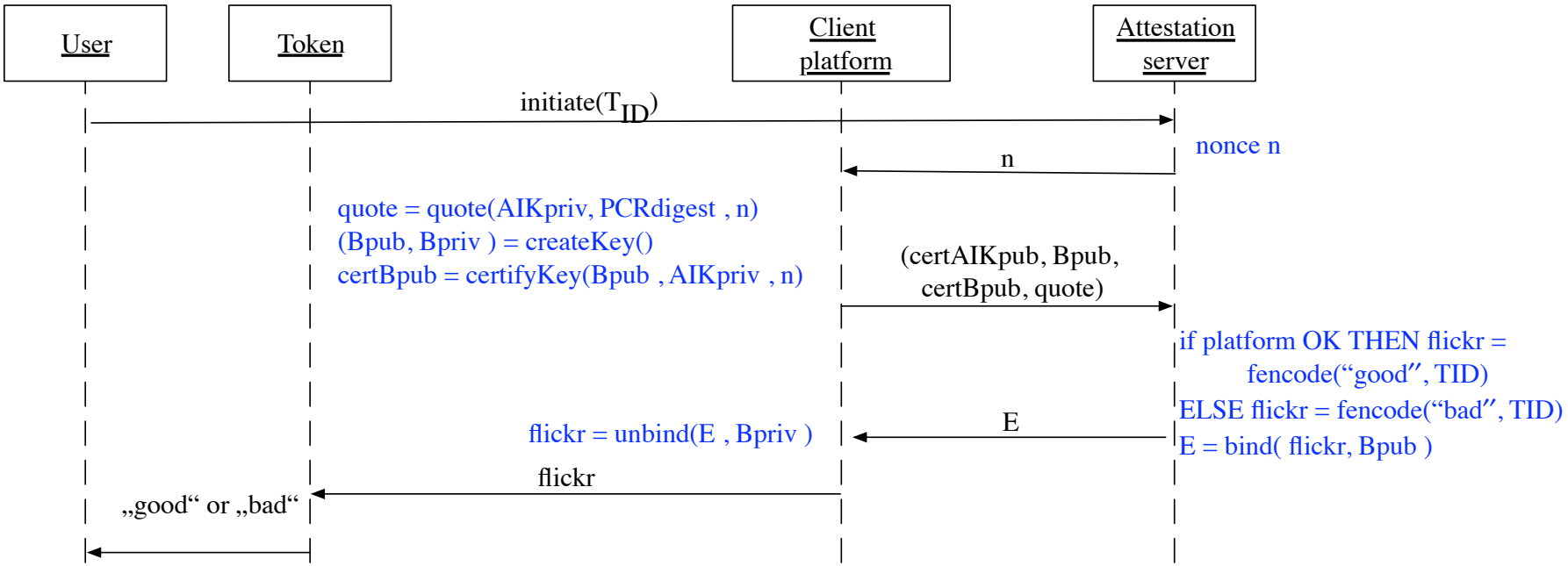
☑ Management and evaluation of integrity measurements

Our ad hoc attestation system – Basic idea (2/2)



- By using encryption, we assert that only "good PC" gets "YES" message
- To this end, in step 2., need to assert that encryption public key comes from the platform being attested
- Security assumption on "good PCs" is that they can keep flickering confidential after decryption
  - Not necessarily the case for PCs running current standard OS (e.g., Windows, Linux, etc)
  - Other protocol variant which works under different assumptions on OS (see paper)

Ad-hoc attestation protocol details (sketch)



Agenda

- Demonstrative ad hoc attestation – idea and challenges
- Token technology
- Our ad hoc attestation system
- Conclusions

Conclusions

- Solved open challenges
- Viable and practically usable solution
- Secure against platform in the middle attacks
- Implementation of demonstrator
- Essentially this work is about reporting attestation results, also works with other attestation technologies (e.g., run-time attestation)
  - Protocols independent of static or runtime attestation
  - Once trusted computing is widespread (?), there is a solution for ad-hoc attestation
- Could also replace token technology with smart-phones based flickering mechanism
  - Problem with smart-phones: open execution architecture, and thus not secure in the long run

Thank you for your attention!