CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

RFID Applications of Embedded Processing and Zero-Knowledge Proof

Robert Winkworth

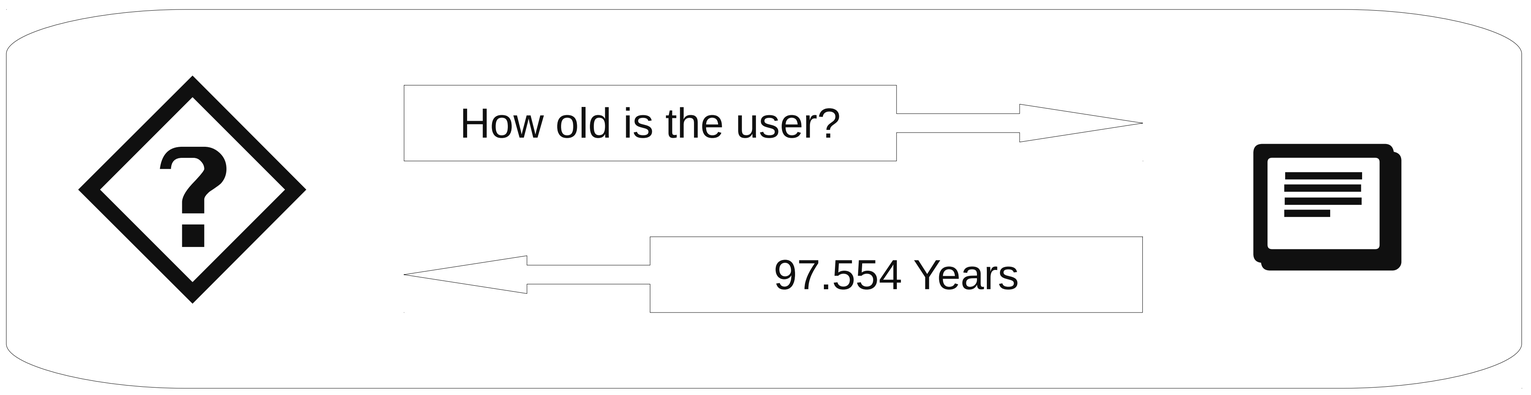
Doctoral Candidate, College of Technology

Like their contact-based predecessors,
devices based on radio frequency identification may be divided into these two categories:

1. **Acquiescent storage** models yield their data to any recognized request.
2. **Embedded systems** process requests, and yield only the resulting output.

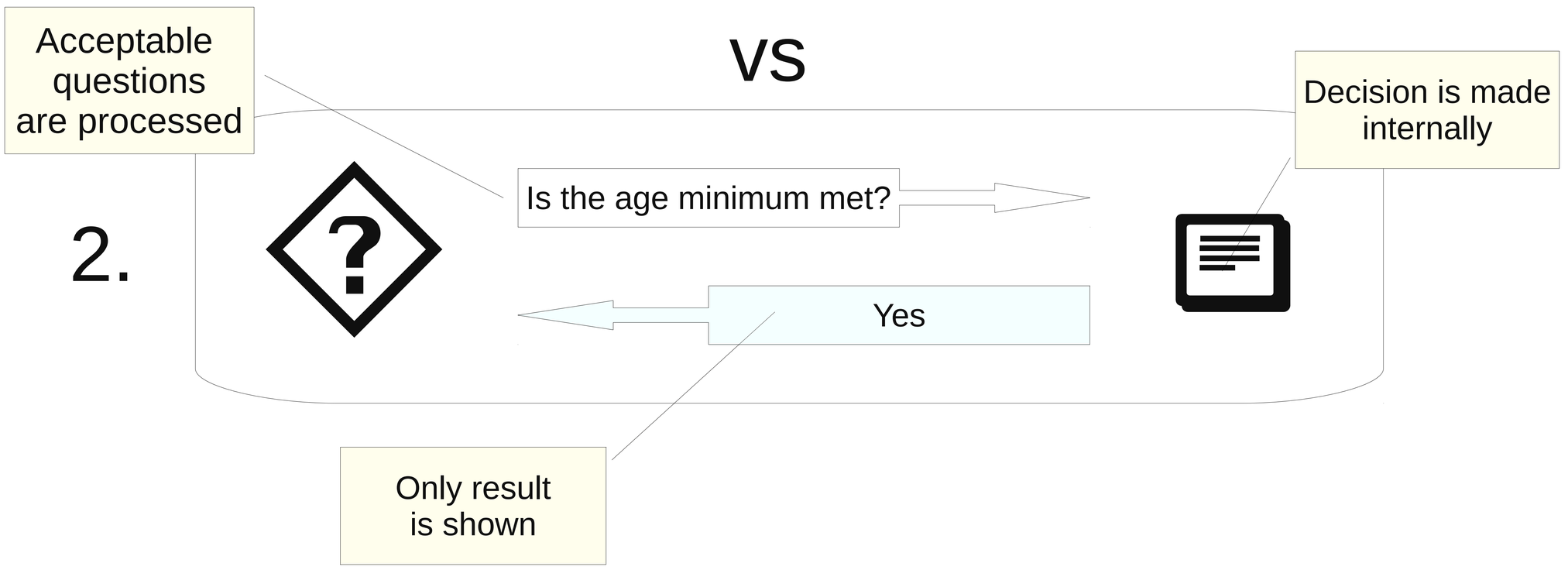
An example that makes the difference clear is the following age-related discount scenario.
In the first case, an RFID card shares information the user might prefer to conceal.
The publicly scan-able transaction between the RFID reader and card looks like this:

1.



VS

2.



The ability to prove data (including credentials) without actually disclosing them makes this technology highly attractive in privacy-sensitive applications, which my thesis work explores in detail.

Live demonstrations of my embedded systems are available on location. See handout for details.

CERIAS

Discovery Park e-Enterprise Center