Combining RFID-Based Physical Access Control Systems with Digital Signature Systems to Increase Their Security

Andrey Larchikov, Sergey Panasenko, Alexander Pimenov, Petr Timofeev

ANCUD, Moscow, Russia

www.ancud.ru   integration@ancud.ru

Main risks of digital signatures

Digital signature systems are adopted worldwide.

However, the following risks must be prevented:

- digital signature secret keys leakage;
- possibility of signing a fraudulent document when a secret key carrier is attached (e. g. due to a virus attack);
- improper or erroneous user behavior that can essentially increase other risks.

Problem: large financial loss

InfoWatch analytic report:

$ 37.8 million of officially claimed direct loss from critical data leakage in the first six months of 2012.

Typical case:

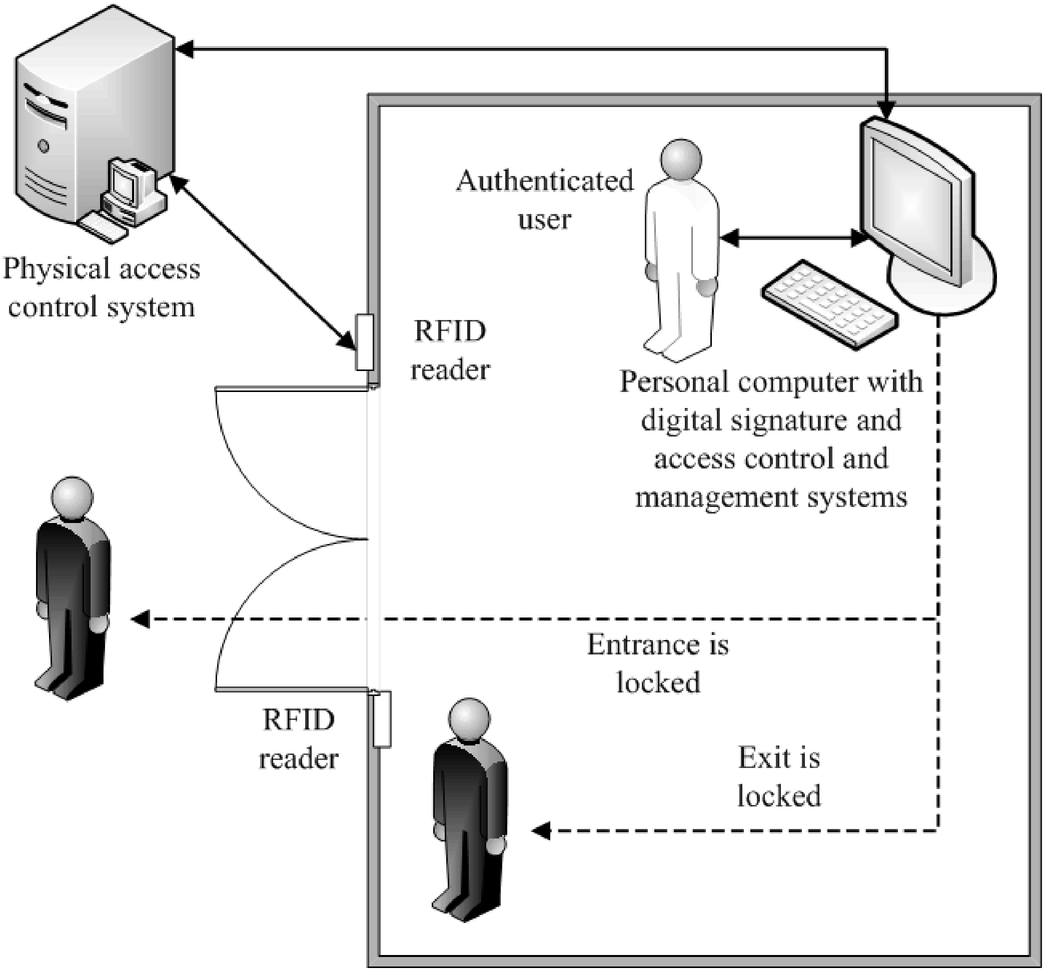
A combination of a virus attack with extremely unprofessional behavior of a digital signature system user led to a RUR 9 million (about EUR 200000) fraudulent money transfer (fall 2013).

How to decrease financial loss

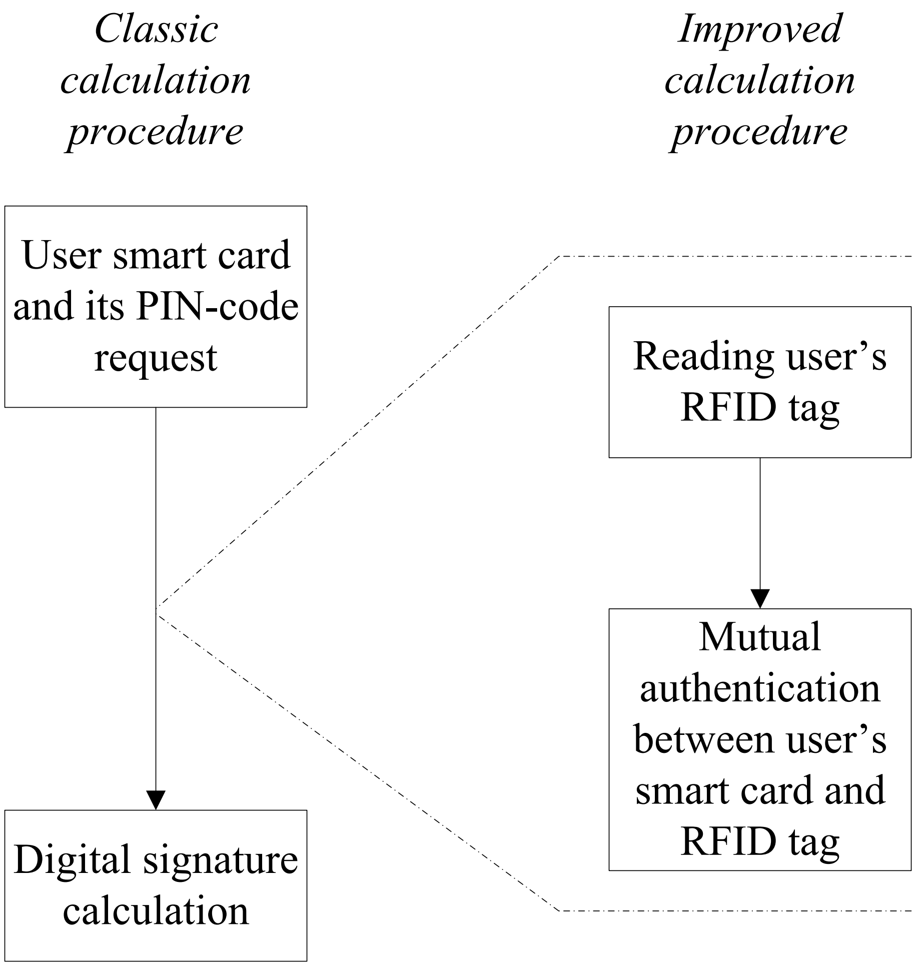
Ways to prevent (or at least decrease) such financial loss:

- by use of strong anti-virus software;
- by signing documents inside smart key carriers with cryptographic functions (smart cards or USB tokens);
- by use of access control and management system with running process inspection and strong user authentication components;
- by combining digital signature systems with physical access control systems.

Combination of digital signature and physical access control systems


Physical access control system
Authenticated user
RFID reader
Personal computer with digital signature and access control and management systems
Entrance is locked
RFID reader
Exit is locked

Next step: involving high-end RFID tag into a digital signature protocol


Classic calculation procedure
Improved calculation procedure
User smart card and its PIN-code request
Digital signature calculation
Reading user's RFID tag
Mutual authentication between user's smart card and RFID tag

Further evolution

RFID tags for physical access control systems can also be combined with a computer access control and management system, e. g.:

- by involving user’s RFID tag into his authentication process to gain access to the computer;
- by permanent monitoring if user’s RFID tag is present at the working area – otherwise the computer can be automatically locked or shut down.

Conclusion

1. Using RFID technology in digital signature schemes allows to increase their security. Even low-end RFID tags can add one more security level when combined with physical access control systems.
2. Intellectual RFID tags with possibility of strong mutual authentication with smart cards allow to prevent unauthorized access to digital signature secret keys: they can be used after successful mutual authentication only.

Thank you!

Andrey Larchikov, Sergey Panasenko, Alexander Pimenov, Petr Timofeev

ANCUD, Moscow, Russia

www.ancud.ru   integration@ancud.ru