Smart Cards

Towards a modern run-time platform

5. Real-Life Application

Thorsten Kramp & Michael Kuyper
IBM Zurich Research Laboratory

Overview

A. BlueZign

replace "legal paper" with electronic documents

B. Biometrics

basics, technologies, identification vs. verification, biometrics and smart cards

A. BlueZign: The Problem

- Replace "legal paper" with electronic documents
- Benefits of converting from paper to digital records
  - *reduced handling costs*
  - *greater efficiency*
  - *greater flexibility*
  - *less prone to human errors*
  - *simpler process integration*
- Regulated environments require legally binding signatures
  - *a laboratory manager accountable for acknowledging drug testing procedures*
  - *a judge being legally responsible for the conveyances he signs*
  - *an aircraft engineer being responsible for FAA procedural compliance*
  - *a broker responsible for SEC compliance*

A. BlueZign: Legal Issues

- Handwriting one's name on paper has been the principal means of signature for centuries
- In an electronic setting, the broad legal definition of signature may include a variety of elements such as scanned images, letter heads, and other electronic representations of paper artifacts
- For digital signatures to fulfil basic purposes of signatures, key characteristics are required
  - *indicate by whom they are signed*
  - *be difficult for somebody to produce without authorization*
  - *identify what is signed*
  - *be difficult to alter without detection*
  - *the action of signing should be an affirmative act indicating approval and authorization*

A. BlueZign: Signature Requirements

- Signatures are bound to people, generated using private keys
  - *desirable that key kept under persons control (privacy, trust)*
    - ☛ implies some form of hardware token (e.g., a smart card)
  - *private keys need to be very secure*
    - ☛ generated on the token, only the public key exported
  - *person needs to authenticate to the card*
    - ☛ password/PIN or biometrics (eg. finger print or iris recognition)
- Signatures must be future proof
  - *RSA key length of ~2500 bits to generate a signature secure for 30 years*
  - *BUT: it makes little sense to look past 10 years in the future*
    - ☛ *system must be upgradeable*

A. BlueZign: Project Example

- GILFAM-AMALFI
  - *digitalization of land registry records in Haut-Rhin, Bas-Rhin, Moselle regions in France*
  - *introduction of electronic signatures for legal conveyances of property*
  - *30 years validity of documents*
  - *37 judges, 2.5 million pages of archived land registry records*
  - *pages scanned, images sent via satellite to be transcribed, images signed and stored*
  - *judges to use smart cards, secure card readers with display, and biometric authentification*
  - ☛ *doing away with hundreds of years of books*

A. BlueZign: GILFAM Trust Requirements

- The person signing a record and the beneficiary of the records must trust the infrastructure

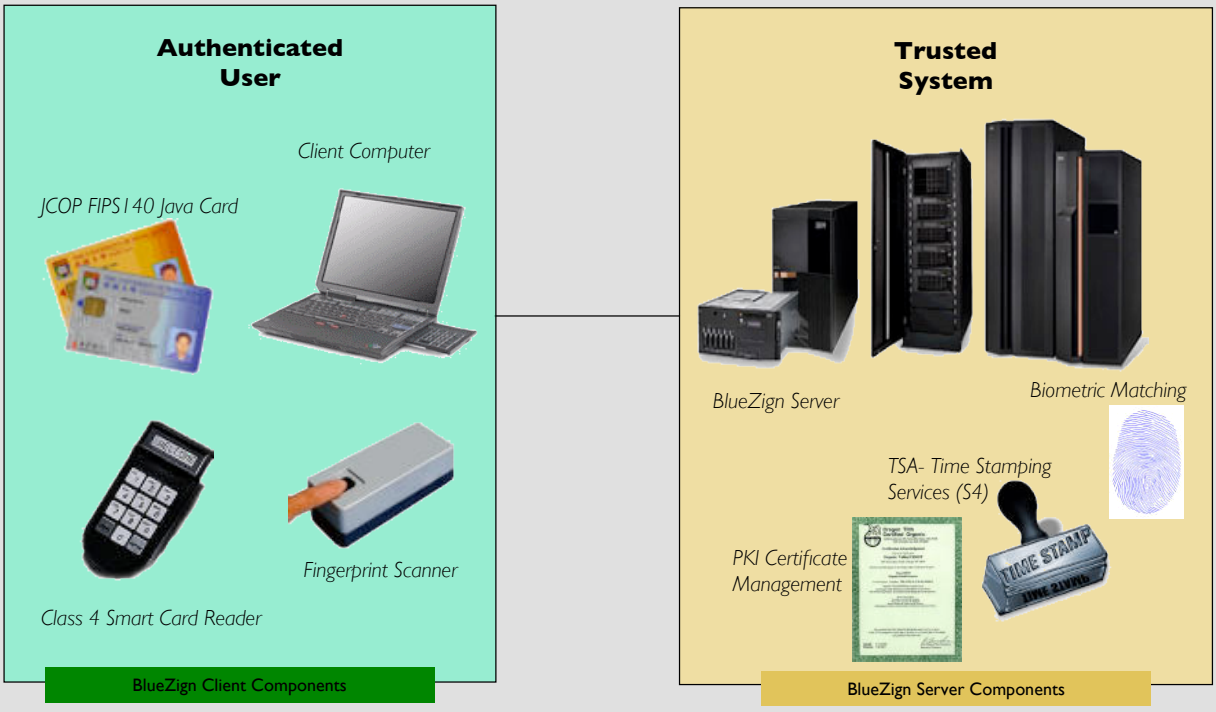
User Requirements

1. *I want to know **what** I'm signing*
2. ***Nobody** else can sign on my behalf*
3. *My signed records **cannot be changed***
4. *I trust in the **future security** of the system*

Beneficiary Requirements

1. *I trust the **integrity** of the system*
2. *I trust in the **future security** of the system*

A. BlueZign: GILFAM Overview



A. BlueZign: GILFAM Flow