





Ray Desrochers
Vice President of Engineering
Keyware Technologies

Facts

Started 1996
Boston/Brussels
200 people
>1000 customers
Nasdaq Europe
[KEYW]
23 June 2000

The mission

“Establish Keyware
as a leading
Security Access
and Biometric enabling
company”



Authentication Issues

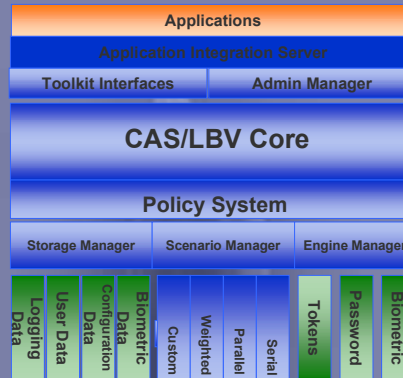
- Authentication, the foundation of good security
- Many authentication methods
- Many just in biometric authentication
- Need to maximize investment
- Need to minimize risk in picking the wrong solutions
- Need to keep up with change
- Local authentication solutions won't work

CAS™ Central Authentication Overview

- **Central Authentication**
 - Much more secure than local authentication
 - Uses best-of-breed industry solutions
 - Easily take advantage of next-generation offerings
- **Central Administration**
 - Centrally managed platform
 - Fast updates to rules and policies
 - Control down to the individual user level
 - Use existing, centrally protected data stores
 - Supports decentralized authentication using Smart Cards
- **Layered Verification**
 - Combine the best features of all methods
 - Combine methods / technologies for better results
 - Significant advantages over single authentication solutions

CAS Architecture

- Scalable
 - Distributed databases and modules
 - Threaded processes
- Interoperable
 - Multi-platform support
 - Open development environment
 - Internet, Smart Card, Telephony Toolkits
- Adaptable
 - Layered authentication
 - Custom decision policies

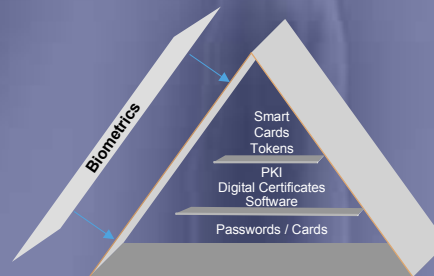


Strong Authentication

Why biometrics?

Biometrics complement existing security systems. In particular, they:

- Enhance security, cannot be stolen or copied
- Increase convenience, cannot be lost or forgotten
- Accuracy dependent on human changes, environmental conditions, application demands, technology (hw/sw)



Biometric Market Drivers

- Growing
 - fear of fraud
 - threat of Identity theft
 - need for privacy
 - high profile security breaches and hacker attacks
- Other authentication methods cannot assure the identity of the user
- Internet applications are driving the need for increased security
- HIPAA
- Infrastructure becoming available at low prices (Webcams, Microphones, silicon fingerprint readers....)

Dutch Burn Institute

- Non-profit organization that conducts research about burn injuries
- Based in the Netherlands
- No good central patient databases until now
- Developing evidence-based treatments is a key goal
- Very few evidence-based protocols currently in use or under development in Europe
- Large samples are required to form conclusions
- Many different groups involved in the process

Business Challenge

- Data collection from regional burn centers
- Need to meet stringent government standards
- Strong authentication for data access
- Simple access for doctors and scientists
- General data security concerns
- Privacy and confidentiality concerns
- Need for non-repudiation

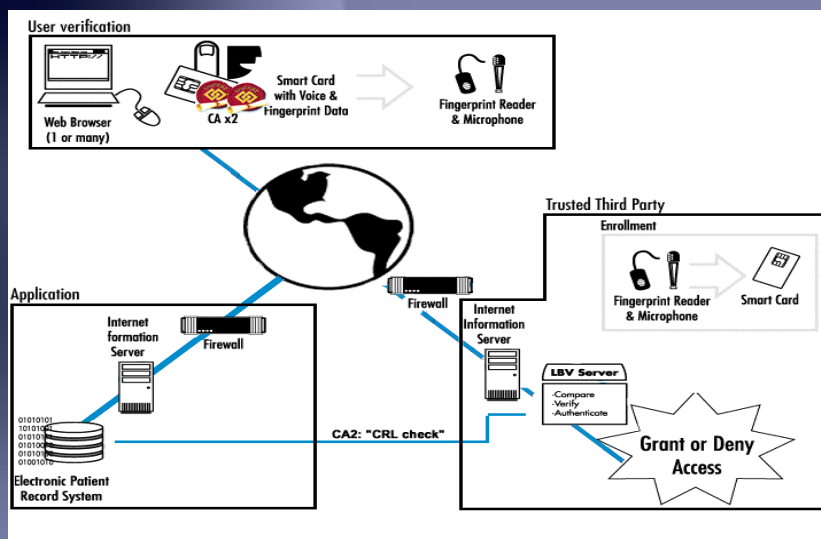
Overall Goals

- High security (guaranteed authentication)
- Privacy (local template storage)
- Trusted third party (TTP) controlling authentication
 - Diginotar (Netherlands digital public notary)
 - Trusted third party certificate authority
 - Issues end-user digital certificates

Overview of the Solution

- Digital Identity, PKI-based, X509v3
- Biometrics: voice and fingerprint
- Use of a smart card for storage of digital identity and biometrics templates
- Activation of digital identity based on biometrics
- Different domains only accessible via exchange key
- Encryption between all devices
- Encryption of database records

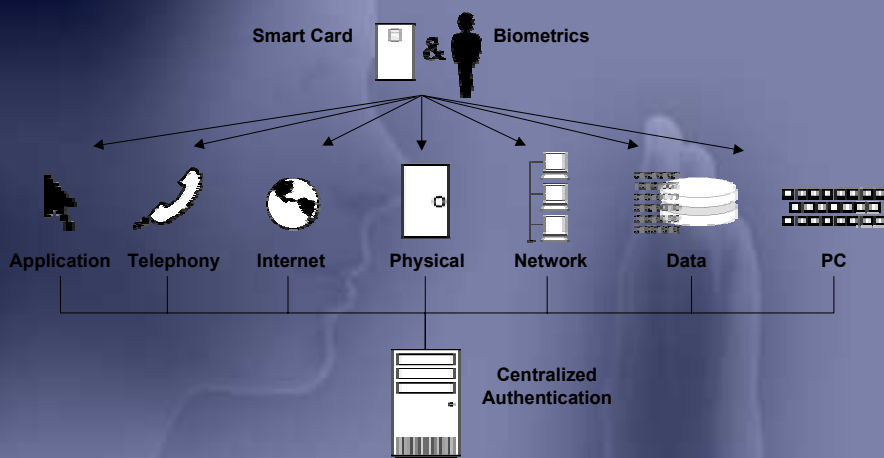
Overview of the Solution



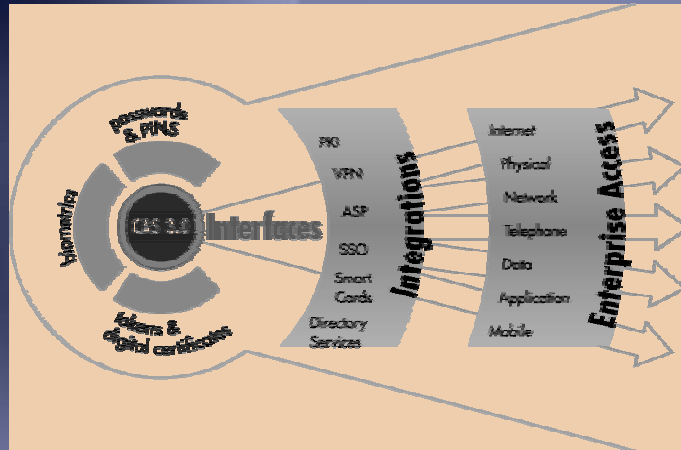
Important Points

- No storage of “live” sample data by Diginotar
- Secure yet simple access by users
- Solution can scale to meet future needs
- Other biometrics can easily be added for additional security and convenience
 - Face
 - Iris
 - Signature
 - More ...

The Future of Enterprise Authentication



The Future of Central Authentication



 **Keyware**

Questions?



Keyware

www.keyware.com