

genkey

Biocryptics – Offline and Online use case
scenarios

Presentation to Turbine Workshop Jan 2011

Presentation of genKey Deployments

- Example projects
- Biocryptics – overview
- Biocryptic authentication modes
- Offline verification with FlexKey
- Remote online verification using Central Biometric Authentication Service (C-BAS)
- Conclusions

Example projects and experiences

GenKey Example Projects

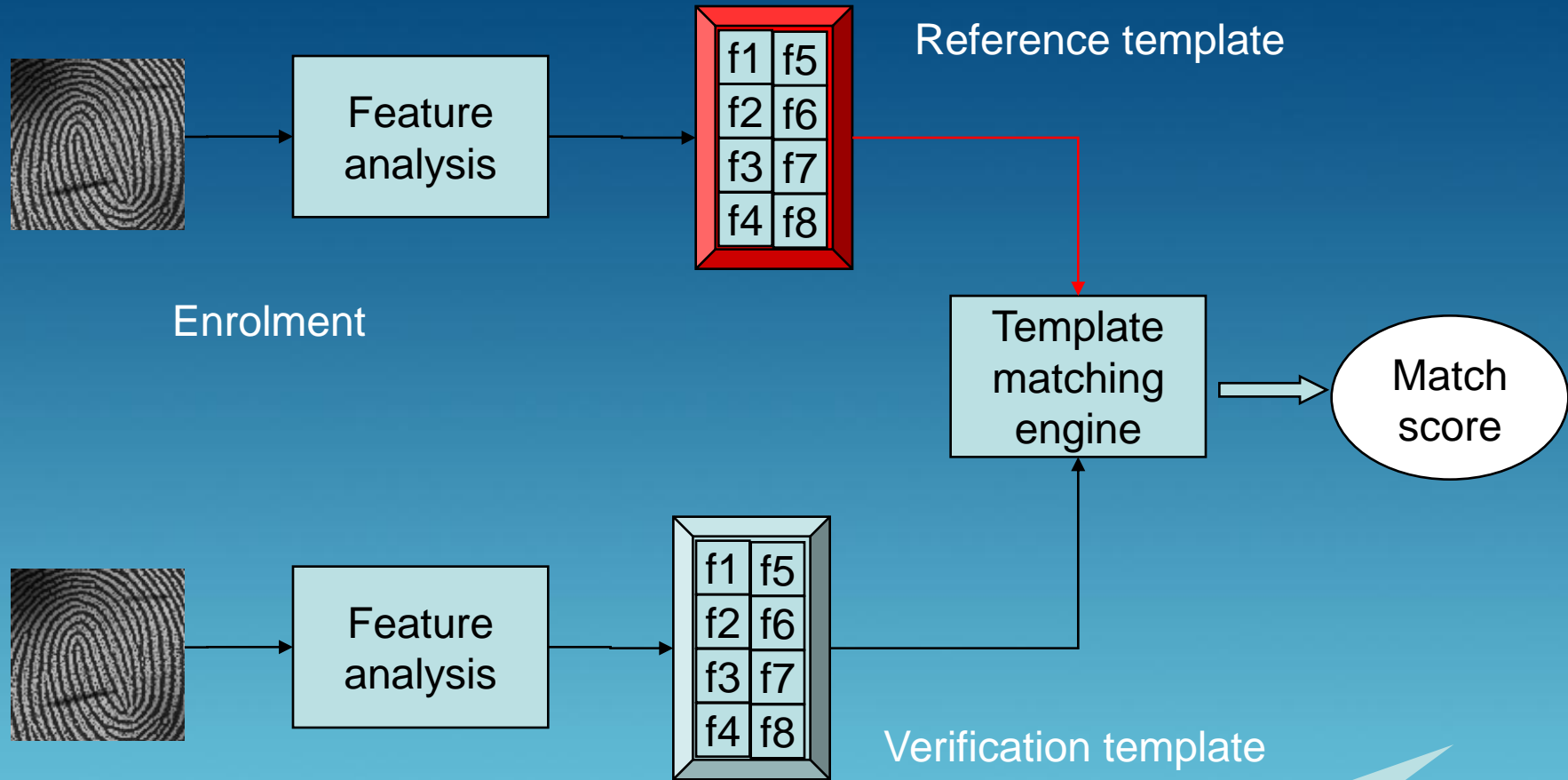
- Licensing of rickshaw owners
- Vehicle licensing
- Facilities access in secure Government building
- Biometric boarding on flights
- Attendance verification and SMS notification in a school
- Student management, exam attendance and fraud elimination

Example projects continued

- Single sign-on within large enterprise
- Vaccination tracking for infant care in developing countries
- eGovernment project Nigeria
- Ghost workers and corruption
- Gun control

Biocryptics Overview

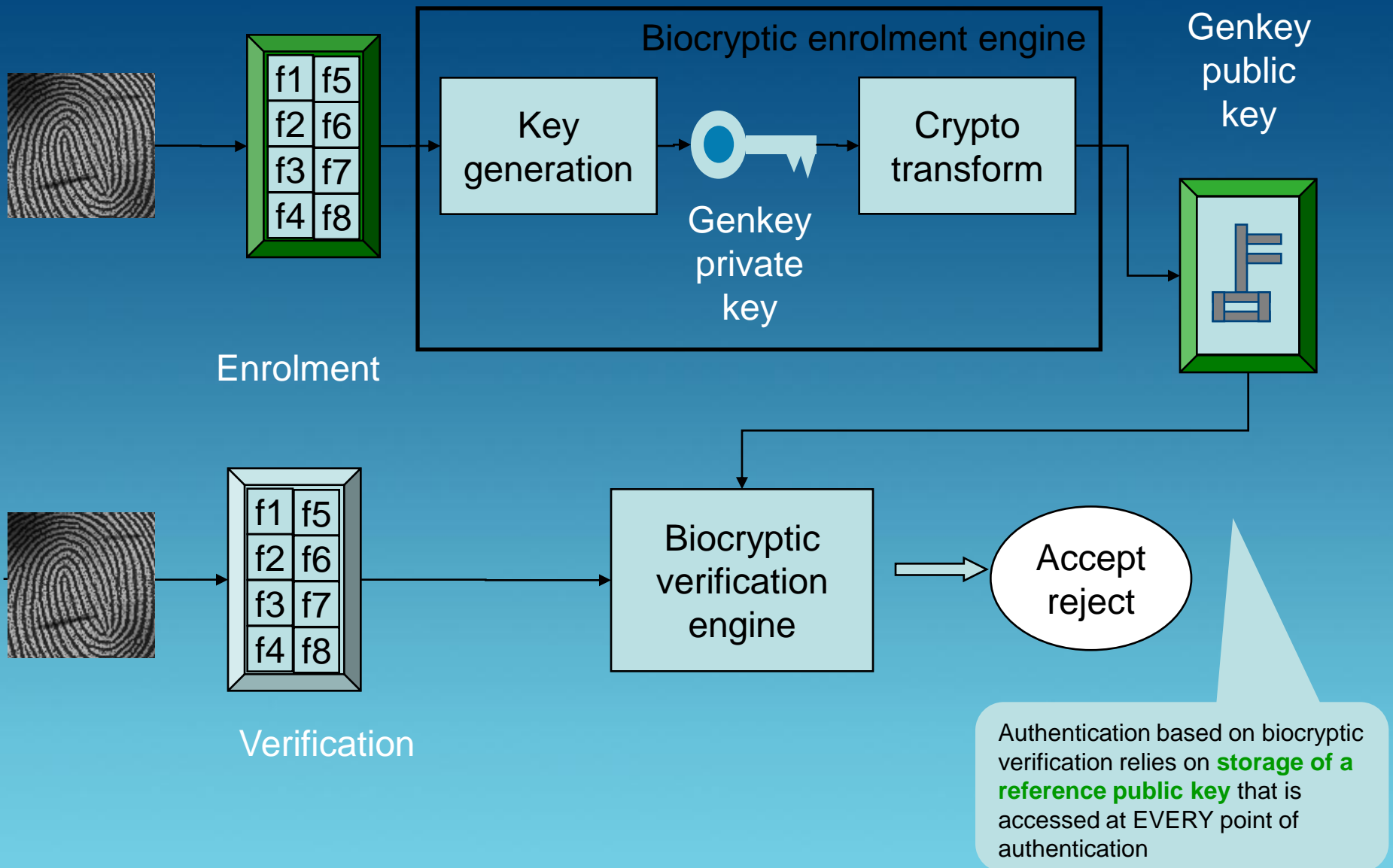
Authentication with templates



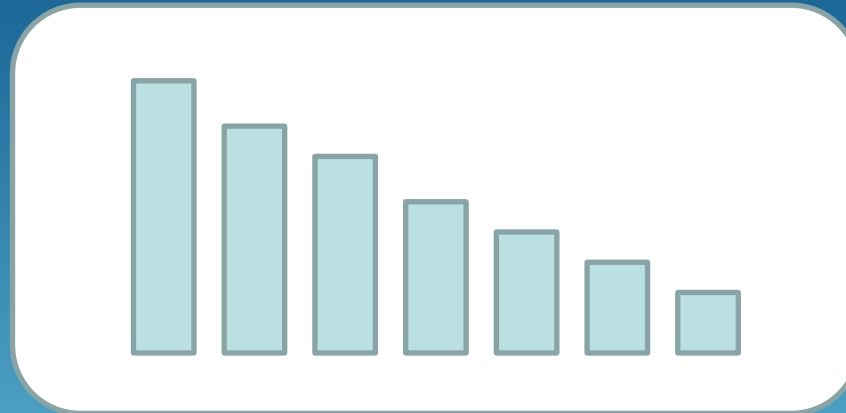
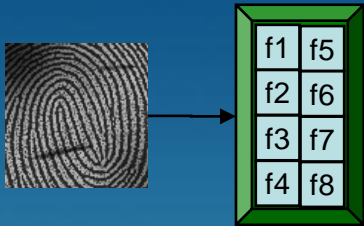
Authentication based on template matching requires **storage of reference biometric data** that **MUST** be accessed at EVERY point of authentication

Authentication with biocryptics

genkey



GenKey Feature Extraction



Stable structure containing a finite set of attribute values which can be ranked based on their usefulness for discrimination.

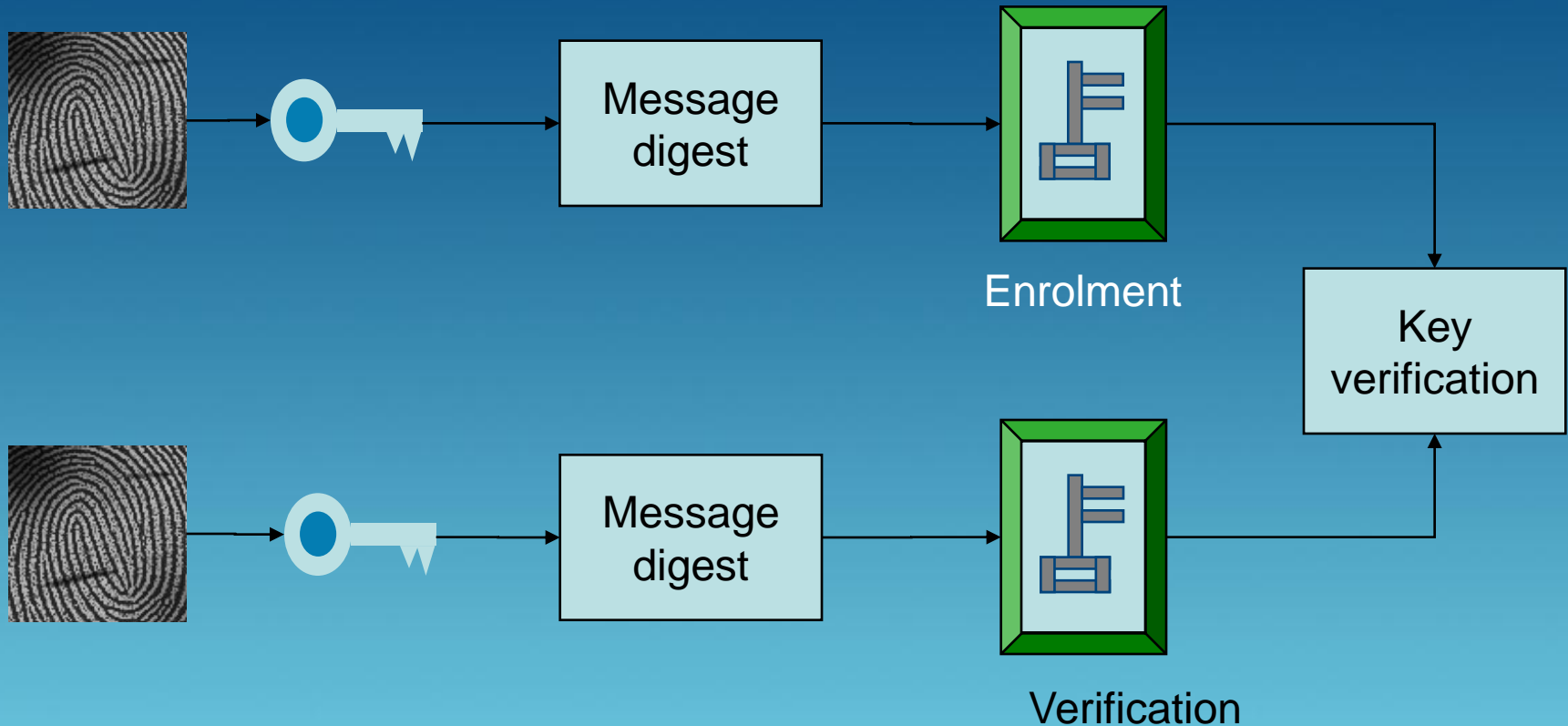
Challenges for key generation

- Minimum threshold of image that must be present to support regeneration of key
- Minimum threshold of image area that must be present to enable a stable spatial reference
- High sensitivity to plastic distortion effects from rolling and twisting of finger
- Excessive finger damage can lead to FTE
- Most issues of image quality are addressable by guiding user behaviours

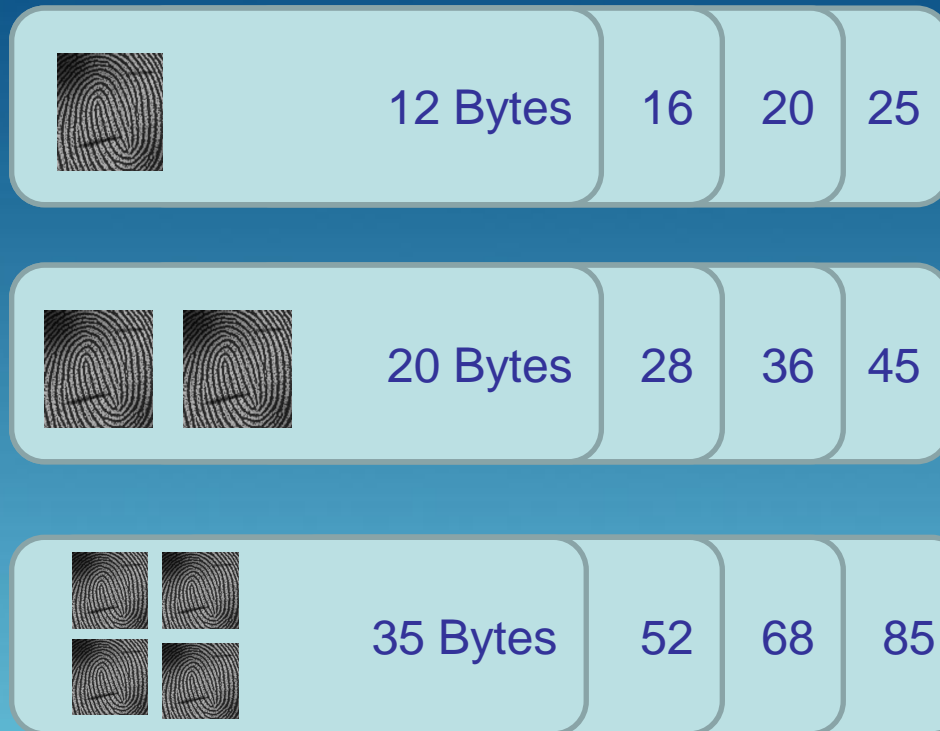
Modes of biocryptics

- Zero storage - One way transform for offline checking of secure documents
- Zero knowledge - Biometric challenge response for remote online verification

Zero storage using one way transform



FlexKey



Compact , self optimizing, low cost, privacy friendly secure solution for offline verification maximising trade offs between storage capacity and performance

Construction of 2 finger FlexKey



Selecting only the most discriminating features allows construction of more compact keys with gentle degradation of accuracy

Applications of FlexKey

- Financial inclusion - Digitally signed 4-finger key within unused third stripe of magnetic stripe cards
- Low cost secure document issuance for colleges : 1D Barcode cheaply printable and readable from secure document as part of low cost issuance process
- Key features:
 - Supports secure offline verification
 - Minimal storage requirement and easy replication
 - Accurate with very fast matching, more than 100,000 matches per second

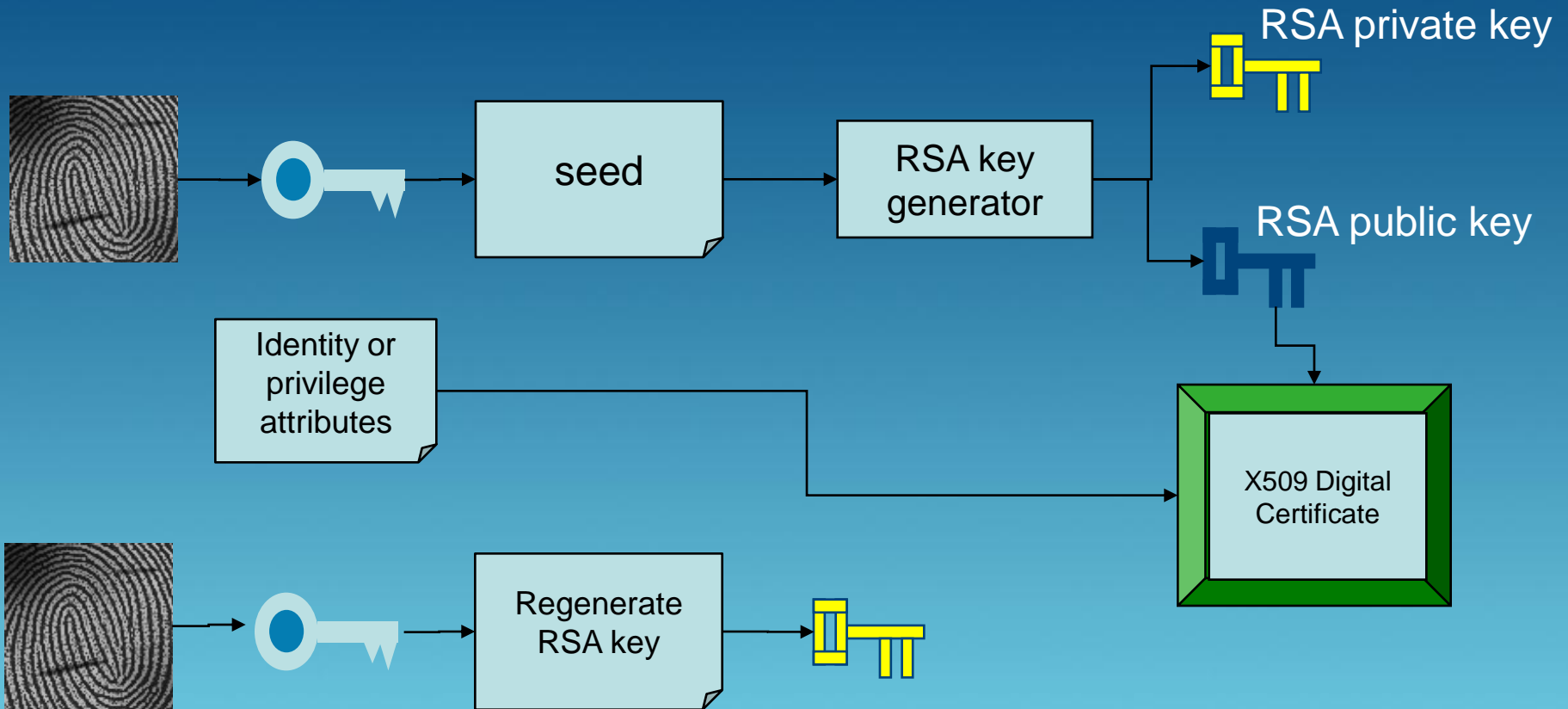
Special case for fast filtered fusion



Applying entropy filtering across a set of multiple fingers facilitates high speed search as pre-filtering step in match engines

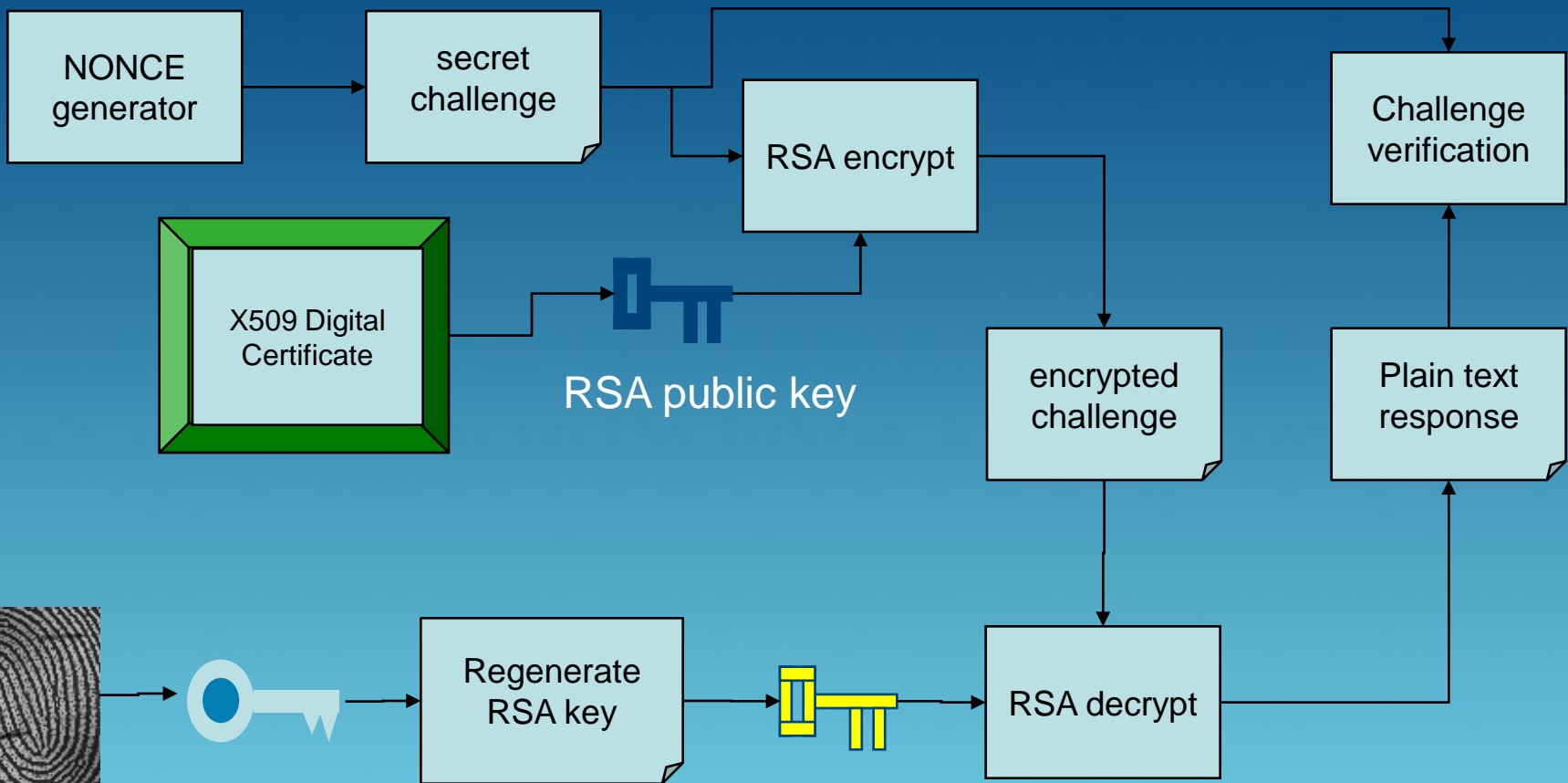
Zero knowledge protocol for online use

PKI Challenge response - issuance



Genkey enables the regeneration of an *arbitrary* private key. This can be linked to a digital certificate using standard PKI issuance process.

PKI Challenge response - verification



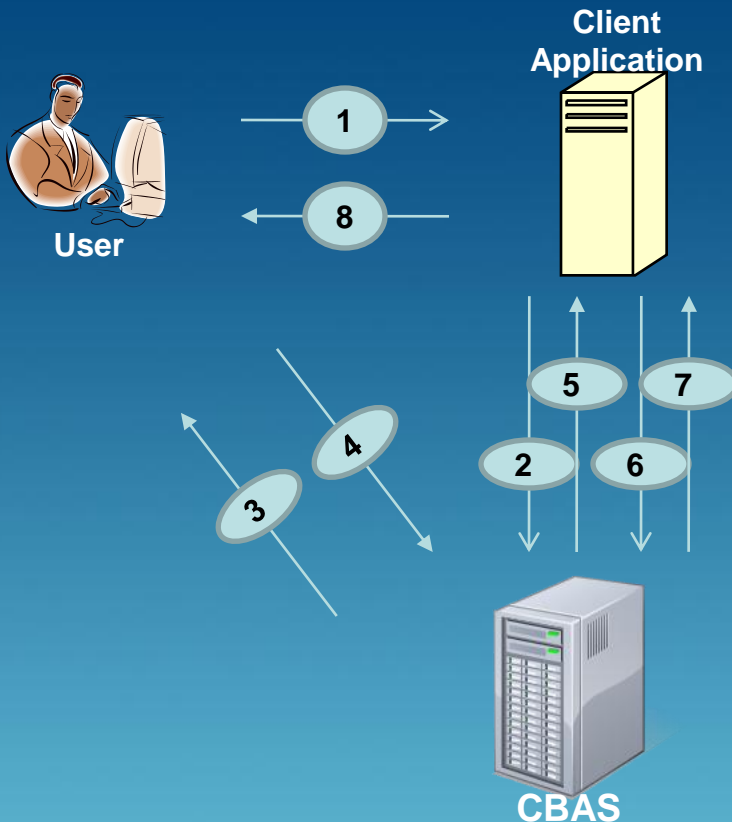
Use of the Genkey enabled private key can be used in a zero knowledge authentication protocol. Relying party only ever has access to RSA public key, which has no mathematical relationship either to the Genkey or the source biometric.

GENKEY C-BAS



enterprise-level, multi-factor, multi-level, biocryptic authentication as a single sign-on, centralized service

CBAS-Simplified Login Flow



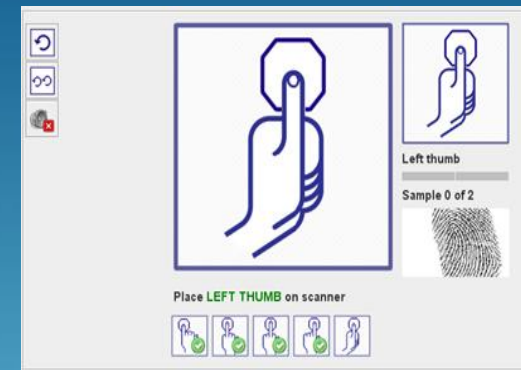
1. User sends request for protected resource
2. Client App authentication request to CBAS (including requested level and resource information)
3. (if user is not already logged in on that level)
CBAS sends credential request for the requested level (e.g. userid/password screen, fingerprint capture request etc.)
4. User returns collected credentials (userid/password, biocryptic key, ...)
5. CBAS validates credentials and send service ticket back to Client Application
6. Client Application performs ticket validation, sending a validation request to CBAS
7. CBAS validates ticket and returns
8. Client Application returns protected resource to user

Note that interaction between client application and CBAS is transparent to the User.

From the User perspective the login flow is equivalent to a typical interaction with a protected resource.

CBAS-Biocryptic Image Acquisition

- ❑ User side component for biometric image acquisition and processing
- ❑ Self-contained service component invoked automatically by user browser for biometric authentication
- ❑ High-speed, high-quality image acquisition for a variety of image capture devices
- ❑ Focus on high-usability for untrained users in self-service/kiosk mode
- ❑ Secure in-depth image analysis including live-detect mode and biocryptic key generation



Application of C-BAS

- Enables biometric credential checking within existing applications with minimal change
- Specifically designed to support remote unattended verification of physical presence
- Implements multi level hierarchical credentials checking infrastructure, with zero exposure of biometric credentials.
- Built using standard protocols, as an extension of the CAS single sign on protocol, and interoperable with existing authentication infrastructure such as LDAP, AD, X509 etc
- Extensible to OpenID, Shibboleth and SAML

Conclusions

- Combination of light weight low cost infrastructure and enhanced privacy eases entry to markets that templates cannot reach
- Successful incorporation of biometrics in a networked environment must be seamless
- Active management of enrolment quality image acquisition process has high impact on operational experiences
- Minimize and simplify the integration pain with external systems – services not components